تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات

(دراسة تحليلية مقارنة)

إعداد

الدكتور/ حاتم أحمد محمد بطيخ

دكتوراه في الحقوق – جامعة عين شمس

أستاذ القانون المنتدب بالجامعات المصرية

﴿ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ

وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي

بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ ﴾

(من سورة النمل الآية: ١٩)

المُلخــص:

نعيش اليوم عصراً جديداً من التقدم العلمي والتقني في مجال تكنولوجيا المعلومات والاتصالات نتج عنه إحداث ثورة تنموية بشرية على جميع المستويات والأصعدة المحلية والعالمية، وأصبحت عملية تبادل المعلومات والمعارف تتم بسهولة ويسر، كما أدي هذا الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة إلى تدفق المعلومات والأخبار والمعارف وتبادل المحادثات بحرية وسلاسة، وعلى جانب أخر فقد خلف هذا التطور التكنولوجي العديد من المخاطر والأضرار لا سيما وضعف الرقابة عليها مما أدي إلى ظهور نوع جديد من الجرائم المتطورة والتي تختلف عن سابقتها من حيث طريقة وأسلوب ارتكابها، وشكل وصفات المجرم وطباعة سميت بجرائم التقنية المعلوماتية، وأصبحت تمثل تهديداً مباشراً وواضحاً للأمن والاستقرار المحلي والعالمي، وعائقاً يحول دون إتمام عملية التطوير والتنمية الاقتصادية والأمنية. وإزاء ذلك سعت العديد من الدول إلى تطوير نظمها التشريعية بإدخال نصوص وتشريعات عقابية وإجرائية تتوافق مع ظاهرة الإجرام التقني الحديثة، ومن هذه التشريعات ما كان موفقاً ومنها ما أصابه بعض الخلل والقصور، وهو ما سنعالجه تباعاً ويكون محلاً للدراسة والتحليل البحثي المقارن .

الكلمات المفتاحية:

تكنولوجيا المعلومات– الإجرام التقني الحديث– المكافحة التشريعية.

Summary:

Today we live in a new era of scientific and technical progress in the field of information and communication technology, which has resulted in a human development revolution at all local and global levels. The process of exchanging information and knowledge has become easy and smooth, and this rapid spread of information through various means of communication has led to the flow of information, news and knowledge. The exchange of talks freely and smoothly. On the other hand, this technological development has left many risks and damages, especially the weakness of oversight over them, which led to the emergence of a new type of advanced crimes that differ from the previous ones in terms of the method and method of committing them, and the form and characteristics of the criminal and the printing of so-called IT crimes It has become a direct and clear threat to local and global security and stability, and an obstacle to the completion of the process of development, economic and security development, and in view of this many countries have sought to develop their legislative systems by introducing punitive and procedural texts and legislation that correspond to the phenomenon of modern technical crime. It has some defects and shortcomings, which we will address successively and be the subject of study and analysis Comparative inductive.

key words:

Information technology - modern technical crime - legislative control.

المقدمـــة

أولاً: التعريف بموضوع البحث:

شهد العالم في السنوات القليلة الماضية عصراً جديداً من التقدم العلمي وما صاحبه من تطور ونهضة غير مسبوقة في كافة المجالات الحياتية، وكان من أبرزها التقدم الحاصل في مجال تقنية المعلومات والاتصالات وما ترتب عليه من إحداث ثورة تنموية بشرية على جميع المستويات والأصعدة المحلية والعالمية، فمن خلالها استطاع الإنسان أن يرصد ويتابع كل ما يدور ويجري حوله في جميع أنحاء العالم بالصوت والصورة منذ اللحظة الأولي، وأصبحت عملية تبادل المعلومات والمعارف تتم بسهولة ويسر، كما أدي الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة إلى تدفق المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية بحرية وسلاسة.

وعلى الجانب التشريعي فقد أتاحت كافة الدساتير والمعاهدات والاتفاقيات العالمية والمحلية للإنسان الحرية الكاملة في استخدام وسائل التقنية المعلوماتية وتبادل البيانات والمعلومات ووسائل التواصل الاجتماعي إلا أن هذه الحرية لا ينبغي أن تجعل من الانترنت ووسائل التقنية الحديثة بيئة متحررة من القواعد والنصوص القانونية الحاكمة والمنظمة لها[1]، فإلى جانب المزايا العديدة التي خلفها هذا التطور التكنولوجي الحديث، أفرز لنا الكثير من الجرائم والتعديات التي تختلف في صفاتها وأشكالها وأثارها عن الجرائم التقليدية، وأصبحت تمثل تهديداً مباشراً وواضحاً للأمن والاستقرار المحلي والعالمي، وعائقاً يحول دون إتمام عملية التطوير والتنمية، ولم تقتصر عواقبه وآثاره على المستوي الفردي بل

---

(١) أكدت على ذلك محكمة Pontoise الابتدائية في أحد أهم أحكامها التي صدرت في ٢٠٠٥/٢/٢
TGI Pontoise, 6e ch., 2 février2005: Comm.Com. Electr. 2005, Comm. 35, Ch. Caron: «l'outil exceptionnel de communication et d'échange que représente le réseau internet ne saurait être en tout état de cause une zone de non droit, c'est-à-dire un univers, lieu de liberté où les règles juridiques élémentaires ne s'appliquent pas »

امتدت لتهدد المجتمع الدولي بأكمله، خاصة وأن هذه الطائفة من الجرائم تتميز بأنها معقدة للغاية لتنوعها وسهولة ارتكابها وقدرة الجناة على التخفي والهرب، مما يصعب معه اكتشافها، واثبات أدلتها، وضبط مرتكبها، وإسنادها إليهم.

وكان من أهم العوامل التي أثرت، بل وساهمت في ظهور هذه الجرائم التقنية، وانتشارها بصورة سريعة ومرعبة مما جعلها تجتاح العالم بأثره، التطورات العلمية، والتحولات الاقتصادية والاجتماعية والثقافية العالمية والمحلية، والفراغ الاجتماعي الأسري وغياب القيم والمبادئ الدينية والأخلاقية لدي الأبناء، والبطالة والسعي وراء توفير الاحتياجات المالية بسبب انهيار الاقتصاد وقلة وضعف المرتبات والدخول مما دفع الأفراد إلى البحث عن الوسائل البديلة لتنمية دخولهم وتلبية الاحتياجات المعيشية[1]، وكان من أخطر هذه العوامل وأهمها عدم وجود التشريع المناسب والعقوبة الرادعة نظراً لحداثة هذه الطائفة من الجرائم والمجرمين، واعتماد أغلب الدول على التشريعات التقليدية القديمة التي أصبحت لا تتناسب مع خطورة هذه الطائفة من الجرائم المعلوماتية مما دفع المجتمع الدولي إلى البحث فيما إذا كانت القوانين التقليدية المتعلقة بمكافحة الجريمة كافية لمواجهة ظاهرة الأجرام المعلوماتى التقني والاستخدامات غير المشروعة لتكنولوجيا المعلومات، أم أنها بحاجة لتطوير قواعدها ونصوصها القانونية المعمول بها لمواجهة الجريمة والفكر الإجرامي التقني وسن تشريعات ونصوص عقابية جديدة.

وإزاء ذلك حملت العديد من الدول على عاتقها لواء البحث في هذا الجانب، وحرصت على تطوير نظم المكافحة التشريعية لديها بإدخال نصوص تشريعية

---

(١) د/ صالح سليمان عبد العظيم– الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦– ٢٨ سبتمبر ٢٠٠٤، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الإسلامي، ص٢٥ وما بعدها.

عقابية وإجرائية تتوافق مع ظاهرة الإجرام التقني الحديثة، ولم تكتفي بذلك فحسب بل قامت بسن تشريعات خاصة مستقلة تتعلق بهذا الشأن، خاصة على الجانب التشريعي المصري والعربي، ففي مصر صدر القانون رقم ١٧٥ لسنة ٢٠١٨[١] ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠[٢] بشأن مكافحة جرائم تقنية المعلومات، ولم يكن هو الخطوة الأولي في مجال التشريع المعلوماتى، بل سبقه العديد من الاجتهادات التشريعات التي تناولت تنظيم مجال التقنية المعلوماتية كان من بينها قانون حماية الملكية الفكرية، وقانون التوقيع الالكترونية، وقانون تنظيم الاتصالات وتكنولوجيا المعلومات، ولم يقف الأمر عند هذا الحد فقط، بل لقد كان حرص المشرع المصري في هذا الشأن عظيماً وضمن بنصوص الدستور المصري الصادر عام ٢٠١٤ العديد من النصوص التشريعية المتعلقة بتنظيم تقنية المعلومات.

وعلى جانب التشريعات العربية المقارنة أصدرت دولة الكويت القانون رقم ٦٣ لسنة ٢٠١٥[٣]، ودولة الأمارات العربية المتحدة بإصدارها القانون الاتحادي رقم ٥ لسنة ٢٠١٢ وتعديلاته[٤]، والمملكة السعودية بإصدارها نظام المكافحة المعلوماتية[٥]، وتعد هذه الخطي التشريعية الحثيثة وبحق انعكاس صادق لعمق المشكلة التقنية والممارسات غير المشروعة لوسائل التقنية المعلوماتية بما تمثله من تهديد حقيقي لحقوق جديرة بالحماية القانونية.

---

(١) منشور بالجريدة الرسمية– العدد ٣٢ مكرر (ج) بتاريخ ٨/١٤ /٢٠١٨.

(٢) منشور بالجريدة الرسمية في العدد ٣٥ تابع (ج) – بتاريخ ٢٧ أغسطس سنة ٢٠٢٠.

(٣) صدر بقصر السيف في ٢٠ رمضان ١٤٣٦– الموافق ٧ يوليو ٢٠١٥ ليعمل به بعد ستة أشهر من تاريخ نشره في الجريدة الرسمية.

(٤) المنشور بالجريدة الرسمية العدد (٤٥٠) ملحق السنة الثانية والأربعون– بتاريخ ٢٠١٢/٨/٢٦، والمعدل بموجب المرسوم بقانون الاتحادي رقم ٢ لسنة ٢٠١٨.

(٥) صدر بموجب قرار مجلس الوزراء رقم ٧٩ بتاريخ ١٤٢٨/٣/٧ هـ، والمصدق عليه بالمرسوم الملكي رقم ١٧م بتاريخ ١٤٢٨/٣/٨، والصادر بالقرار رقم ١١٥٦٧/ ب– بتاريخ ١٤٢٨/٣/٩ هـ.

ثانياً: أهمية البحث:

تبرز أهمية هذا البحث في كونه محاولة من الباحث لتسليط الضوء على ظاهرة الإجرام التقني باعتباره ظاهرة مستحدثة لاتزال فى حاجه ماسة الى مزيد من البحث والدراسة خاصة مع ظهور هذه الجرائم بشكل واضح ومنتشر في العديد من المجالات وعلى جميع المستويات والاصعدة.

كما تكمن أهمية هذه الدراسة في أنها تقدم دراسة عامة تحليلية لنصوص قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية من الناحيتين الموضوعية والإجرائية، وقد اعتمد الباحث في هذه الدراسة على الإسلوب التحليلي المقارن ببعض النصوص والتشريعات العربية والاوروبية بغرض التحقق من مدي كفاية هذه النصوص في مكافحة ظاهرة الإجرام التقني، والتعرف على أهم الضوابط وسبل وآليات التعاون الدولي في مجال مكافحة هذه الجرائم.

ثالثاً: أهداف البحث:

هذا البحث هو دراسة تحليلية مقارنة لنصوص قانون مكافحة جرائم تقنية المعلومات ولائحته التنفيذية من الناحيتين الموضوعية والإجرائية بهدف التعرف على أهم المزايا التى تضمنها هذا القانون، والتوصل الى أوجه القصور التى شابت نصوصه بالمقارنة بالنصوص والقوانين الأخري الصادرة في ذات الشأن، وكذا التعرف على أهم الأسس والضوابط المتعلقة بالتعاون الدولي في مجال مكافحة الجرائم التقنية، والنظر فيما إذا كانت هذه التشريعات موفقه وكافية من عدمه، ومدي توافقها مع المعاهدات والاتفاقيات الدولية التي أبرمت في هذا الشأن.

رابعاً: منهج البحث:

سنتناول موضوع الدراسة من خلال المنهج التحليلي المقارن باعتباره المنهج الأكثر انسجاماً مع طبيعة وأهداف هذا البحث من خلال استقراء وتحليل الأحكام الواردة في قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨

وبعض الدول المقارنة وفقاً لحاجة البحث ولخدمة أهدافه، ونعرض لأوجه القصور التي شابتها، وطرق معالجتها من خلال طرح عدد من التوصيات الهامة.

خامساً: خطـــة البحـــث:

وللإحاطة بموضوع البحث فقد قمنا بتقسيمه إلى ثلاث مباحث رئيسية، يتفرع عن كل منهم ثلاثة مطالب فرعية كما يلي:

المبحث الأول: نظرة عامة حول قانون تقنية المعلومات وضوابط التعاون الدولي.

- **المطلب الأول: ماهية جرائم تقنية المعلومات.**
- **المطلب الثاني: الجهود التشريعية المبذول لمكافحة الجريمة التقنية.**
- **المطلب الثالث: ضوابط التعاون الدولي وتحديد الاختصاص القضائي.**

المبحث الثاني: أنماط الجرائم وحدود العقوبات المقررة لها .

- **المطلب الأول: جرائم الشبكات وأنظمة وتقنيات المعلومات.**
- **المطلب الثاني: الجرائم المتعلقة بالبريد الإلكتروني والمواقع أو الحسابات الخاصة.**
- **المطلب الثالث: جرائم الاعتداء على حرمة الحياة الخاصة وانتهاك الخصوصية.**

المبحث الثالث: الأحكام الإجرائية الخاصة بمكافحة الجرائم التقنية .

- **المطلب الأول: إجراءات جمع الأدلة والاستدلالات التقنية.**
- **المطلب الثاني: التدابير والإجراءات التحفظية والعقوبات التبعية.**
- **المطلب الثالث: الأحكام العامة المتعلقة بالعقوبة.**

المبحث الأول

نظرة عامة حول قانون تقنية المعلومات

وضوابط التعاون الدولي

تمهيد:

مع ظهور وسائل تقنية المعلومات بميزاتها المتعددة العابرة للحدود الجغرافية والسياسية والثقافية والدينية، أصبحت الحدود الدولية والسيادة الوطنية معرضة للانتهاك والمراقبة، وزادت حالات الاختراق الأمني من خلال عمليات التجسس والإرهاب الالكتروني، والاقتصادي، وبث الشائعات، والأخبار الكاذبة لإحداث البلبلة بين أفراد المجتمع، وإزاء ذلك كان من الضروري الإسراع نحو إيجاد مواجهة تشريعية تتناسب وتلاءم هذا التطور التقني وما صاحبه من تطور في عالم الجريمة والتصدي لمثل هذه الانتهاكات سالفة البيان والحد من التعدي علي وسائل التقنية الحديثة.

وبطبيعة الحال لا جدال في أنه لا يمكن الخوض في دراسة هذه المشكلات وسبل مواجهتها تشريعياً قبل إلقاء نظرة عامة حول قانون مكافحة جرائم تقنية المعلومات والتعرض لأهم الأحكام العامة للقانون فيما يتعلق بماهية جرائم تقنية المعلومات، وعرض أهم الجهود التشريعية المبذولة في هذا الشأن التقني، ثم بيان أهم الضوابط المتعلقة بالتعاون الدولي، وهو ما سنبينه تفصيلاً فيما يلي.

تقسيم:

سوف نقوم بتقسيم دراسة هذا المبحث إلى ثلاث مطالب كما يلي:

المطلب الأول: ماهية جرائم تقنية المعلومات.

المطلب الثاني: الجهود التشريعية المبذول لمكافحة الجريمة التقنية .

المطلب الثالث: ضوابط التعاون الدولي وتحديد الاختصاص القضائي.

المطلب الأول

ماهية جرائم تقنية المعلومات

تمهيد:

ذهب أغلب الفقه القانوني إلي استخدام مصطلح جرائم تقنية المعلومات أو الإجرام المعلوماتى المرافق لظاهرة التطور التكنولوجي لوصف الظاهرة الإجرامية الحديثة المرتكبة من خلال وسائل التقنية المعلوماتية، أو لمجرد التعبير عن الأفعال غير المشروعة المرتبطة بنظم الحوسبة ووسائل الاتصالات التي تتكون عناصرها من وسائل إليكترونية سلكية ولا سلكية، الأمر الذي حدا بنا ضرورة التعرف على ما هو المقصود بهذه الجرائم التقنية ولكن قبل التطرق لذلك رأينا ضرورة تناول تعريف المقصود بمصطلح تقنية المعلومات، وهو ما سنبينه تفصيلاً من خلال التقسيم التالي.

تقسيم:

سوف نقوم بتقسيم هذا المطلب إلى فرعين على النحو التالي:

الفرع الأول: المقصود بتقنية المعلومات.

الفرع الثاني: المقصود بجرائم تقنية المعلومات.

الفرع الأول

المقصود بتقنية المعلومات

استعمل مصطلح تقنية المعلومات في الآونة الأخيرة على نطاق واسع نظراً للتطورات التي حدثت في مجال تكنولوجيا المعلومات، ويقصد به علم المعلومات العلمية، أو علم التعامل المنطقي مع المعلومات وفق ضوابط ونصوص حاكمة

ومنظمة لاستخدامها[١]، أو هي التزاوج والالتحام بين تقنيات الحاسبات والاتصالات والاستعمال المتزايد للالكترونيات في العمليات الصناعية والتجارية ابتداء بنظم البرمجيات (الإنسان الآلي المبرمج) بالحاسب حتى بطاقة الائتمان (الدفع الالكتروني) التي يحتفظ بها المستهلك معه[٢]. وهناك من عرفها بأنها علم التعامل العقلاني، على الأخص بواسطة آلات أوتوماتيكية، مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للاتصالات في ميادين التقنية والاقتصاد والاجتماع[٣].

كما جاء تعريف تقنية المعلومات في المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[٤] بأنها " أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفقاً للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة ".

وعلى الجانب التشريعي فقد عرفتها المادة الأولي من القانون المصري بقولها، تقنية المعلومات هي أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة

---

(١) أ/ محمد على سكيكر – الجريمة المعلوماتية وكيفية التصدي لها– مطابع دار الجمهورية للصحافة، أكتوبر ٢٠١٠، ص١٢.

(٢) د/ هشام فريد رستم– قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، ١٩٩٤، ص٢٨.

(٣) محمد على سكيكر – الجريمة المعلوماتية وكيفية التصدي لها، مرجع سابق، ص١٥.

(٤) تم توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، في القاهرة في ٢٠١٠/١٢/٢١، ووافقت مصر على الانضمام إليها بموجب قرار رئيس الجمهورية رقم ٢٠١٤/٢٧٦ الصادر بتاريخ ١٩ أغسطس ٢٠١٤ والمنشور بالجريدة الرسمية بالعدد ٤٦ في ١٣ نوفمبر ٢٠١٤، وذلك مع التحفظ على شرط التصديق.

سلكيًا أو لاسلكيًا[١]. وتناولها المشرع الكويتي على أنها هي أداة الكترونية تشمل كل ما يتصل بتكنولوجيا المعلومات ولها قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو كهرومغناطيسية أو ضوئية أو وسائل أخري مشابهة سلكية كانت أو لاسلكية وما قد يستحدث في هذا المجال[٢].

ولا يختلف اتجاه المشرع الإماراتي في تعريف تقنية المعلومات كثيرا عما تبناه المشرع الكويتي، حيث عرفتها المادة الأولي من المرسوم الإماراتي بأنها أداة الكترونية مغناطيسية بصرية، كهروكيميائية، أو أي أداة أخري تستخدم لمعالجة البيانات الالكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الالكترونية أو إيصالها للآخرين[٣]، إلا أن المشرع السعودي قد اتخذ موقفاً مغايراً في سبيل تسمية القانون يؤخذ عليه حيث أطلق عليه نظام وليس قانون، وعلى جانب أخر قام بتصنيف الجريمة على أنها جريمة معلوماتية وليست تقنية معلومات، أي عرفه بنظام مكافحة الجرائم المعلوماتية[٤].

وبغض النظر عن المصطلح التعريفي المستخدم للدلالة على ماهية هذه الجرائم المستحدثة فجميعها تؤدي لذات المعني، وتعد كافة هذه التعريفات القانونية التي قيلت في تعريف تقنية المعلومات – من وجهة نظرنا – من أكثر التعريفات التشريعية وضوحاً وشمولية، على الرغم من أن المشرع المصري كان أكثر

---

(١) المادة الأولي من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، والمنشور بالجريدة الرسمية في العدد ٣٢ مكرر (ج) بتاريخ ٨/١٤ /٢٠١٨.

(٢) المادة الأولي من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥.

(٣) المادة الأولي من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم الاتحادي رقم ٥ لسنة٢٠١٢ وتعديلاته، المنشور بالجريدة الرسمية العدد ٤٥٠ ملحق السنة الثانية والأربعون– بتاريخ ٢٠١٢/٨/٢٦.

(٤) نظام مكافحة جرائم المعلوماتية السعودي، الصادر بقرار مجلس الوزراء رقم ٧٩ بتاريخ ٧/ ٣/ ١٤٢٨ هـ، والمصدق عليه بالمرسوم الملكي رقم ١٧م بتاريخ ١٤٢٨/٣/٨، والصادر بالقرار رقم ١١٥٦٧/ ب– بتاريخ ٩/ ٣/ ١٤٢٨ هـ.

تفصيلاً للوسائل التقنية إلى حد ما، ولكن جميع هذه الاجتهادات جاءت موفقة من ناحية الصياغة والتوضيح لمفهوم تقنية المعلومات وما يتصل بها .

الفرع الثاني

المقصود بجرائم تقنية المعلومات

لم يكن من اليسير على مشرعي وفقهاء القانون التوصل لتعريف جامع مانع متفق عليه لجرائم التقنية المعلوماتية[١]، فهي جرائم من الصعوبة تعريفها أو كما قيل هي جرائم تقاوم التعريف نظراً لما يمر به العالم من تطور يومي على الصعيدين العلمي والتقني في مجال الاتصالات وتكنولوجيا المعلومات وما صاحبها من تطور في شبكة الانترنت وظهور فئات من المجرمين والجرائم المتطورة بتطور تلك التكنولوجيا[٢].

وعلى صعيد ذلك فقد تعددت الجهود المبذولة لمواجهة الظاهرة المستحدثة في الإجرام التقني على المستويين المحلي والعالمي- وهو ما سنتناوله تباعاً فيما بعد- وعلى الرغم من تعدد وتنامي هذه الجهود إلا أنها لم توفق في وضع تعريف محدد متفق عليه حول مفهوم جرائم تقنية المعلومات، وأفرزت لنا هذه الجهود العديد من التعريفات المتنوعة والمتباينة التي تختلف فيما بينها ضيقاً واتساعاً، فمنها ما نظر للجريمة التقنية بحسب محل الواقعة المكونة لها بأنها هي التي تقع على أحد مكونات النظام المعلوماتى، ومنها ما نظر إلى الوسيلة أو الأداة التي ارتكبت بها الجريمة واعتبر الجريمة المعلوماتية هي التي ترتكب بواسطة أحد الوسائل

---

(١) وهو ما أكدته قمة برلين:

«Le sommet de Berlin, relative à la cybercriminalité n' aura permis de dégager qu' une seule certitude, une définition universelle de la cybercriminalité et l'on peut même se demander si une entente sera un jour possible» L'impossible définition universel de la cybercriminalité,

http:// www.vilage -justice.com.

(٢) د/ محمد سامي الشوا- ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤، ص٥ وما بعدها.

والأدوات الالكترونية، أي أن تكون الوسيلة أو الأداة الالكترونية التقنية هي أداة ارتكاب الجريمة أو وسيلتها، ومن هذه التعريفات تعريف الأستاذTOM Forester، والأستاذ Eslie D. Ball بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"[١].

وهناك من اعتمد في تعريفه للجريمة على الضابط الشخصي أو المعرفة الفنية لدي المجرم، وجميع هذه التعريفات عجزت عن وضع تعريف محدد للجريمة التقنية، ولم تتفق في مجملها فيما بينها على تعريف جامع مانع[٢].

وكان من بين هذه التعريفات التي قيلت في هذا الشأن، أنها كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب الآلي وشبكات الاتصالات الخاصة به التي يحميها قانون العقوبات، ويفرض له عقابا[٣]، وكذا التعريف الذي تبناه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين الذي أشار إلى أنها كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أي أنها كل جريمة يمكن ارتكابها في البيئة الالكترونية سواء وقعت عليه أو من خلالها أو بواسطته[٤].

كما عرفتها الاتفاقية الأوروبية للجرائم السيبرانية (اتفاقية بودابست)[٥]، بأنها

---

(1) TOM Forester, Essential problèmes to High-tech Society First MIT Prés édition, Cambridge, Massachusetts, 1989, P. 105.

(٢) يراجع في تعريف الجريمة المعلوماتية: د/ سامي على حامد عياد – الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، ٢٠٠٧، ص٣٥. د/ نائل عبد الرحمن صالح – جرائم الحاسوب في التشريع الأردني، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠، ص٢ وما بعدها.

(٣) أ/ محمد على سكيكر – الجريمة المعلوماتية وكيفية التصدي لها، مرجع سابق، ص٣٦.

(٤) مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا، خلال لفترة من ١٠ – ١٧ أبريل ٢٠٠٠.

(٥) انعقدت الاتفاقية الأوربية لجرائم الانترنت في بودابست بدولة المجر بتاريخ ٢٠٠١/١١/٢٣ وتعتبر هي الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الانترنت، وقد تم توقيعها من ٣٠ دولة أوروبية بالإضافة إلى أربع دول غير أعضاء في المجلس الأوروبي وهم كندا،

كافة النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية، وصنفت هذه الاتفاقية الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها، والجرائم ذات الصلة بالكمبيوتر، والجرائم المتعلقة بمحتوي الكمبيوتر، والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية.

ومن بين هذه التعريفات أيضاً التعريف الذي ورد في الإجابة البلجيكية على الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية عام ١٩٨٢ حول الغش المعلوماتى، بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[١]. ويعد هذا التعريف الأخير من وجهة نظرنا من أفضل التعريفات التي قيلت في تعريف الجريمة التقنية وأوقعها والتي تمثل تجسيداً حقيقياً للجريمة التقنية على الرغم من اتساعه وشموليته .

ومن هنا فقد فرق الفقه المقارن بين الجريمة المعلوماتية والجريمة الافتراضية، إذ يقول أنه رغم وجود ارتباط بين هاذين النوعين من الجرائم، إلا أن هناك تمييز بينهما يخلص في أن النوع الأخير من الجرائم وهو الافتراضي يتطلب اتصال دائم بالشبكات، أما الجريمة المعلوماتية فالأمر يختلف تمام حيث أن هذه الجريمة قد ترتكب بعيداً عن الاتصال بالشبكات ومنها الانترنت كجريمة العدوان علي حق المؤلف[٢].

الولايات المتحدة الأمريكية، اليابان، جنوب أفريقيا. للمزيد حول هذه الاتفاقية يراجع: د/ عمر محمد أبو بكر يونس– الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، ٢٠٠٤، ص١٩٨-٢٠٠. د/ جورج لبكي– المعاهدات الدولية للانترنت، حقائق وتحديات، مجلة الدفاع الوطني، ص٣، بحث منشور عبر الانترنت على موقع:

http://www.lebarmy.gov.lb.

(١) د/ هشام فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٣٠ وما بعدها.

(2) E.cesay: digital evidence and Computer Crim " londer, academic press", 2000, p.9 et s. & D.parker: Combattre la Criminalite informatique (paris,

أما على الجانب التشريعي فبالرجوع إلى نصوص قانون مكافحة تقنية المعلومات في كل من مصر والإمارات، نجد أنهما لم يتناولا وضع تعريف للجريمة التقنية أو المعلوماتية، لا من قريب أو من بعيد، وعلى العكس من ذلك فقد اتجها كل من المشرعين الكويتي والسعودي اتجاهاً مغايراً وحرصا على وضع تعريف محدد للجريمة المعلوماتية، ففي المادة الأولي من قانون مكافحة تقنية المعلومات الكويتي عرفت الجريمة التقنية بأنها كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون[١]، وعرفها المشرع السعودي بأنها أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام[٢] .

إلا أننا نأخذ على هاذين التعريفين قصورهما وعدم دقتهما، فقد اقتصرا على فعل الارتكاب فقط، ولم يتناولا الامتناع غير المشروع، كما أنهما جعلا المخالفة أو عدم المشروعية قاصرة على ما ورد بنصوص هاذين القانونين فقط دون التطرق لأحكام قانون العقوبات باعتباره الشريعة العامة للعقوبة .

وفي جميع الأحوال، فإننا نري أن ما تبناه كل من المشرع المصري والإماراتي من عدم النص على تعريف محدد لجرائم تقنية المعلومات هو اتجاه صائب ومحمود، حيث أن الرأي الغالب والمتفق عليه لدي جانب عريض من فقهاء القانون أن المشرع ليس مختصاً بوضع تعريف للجريمة، فذلك العمل يدخل في صميم اختصاص ومهام رجال الفقه والقضاء، نظراً لتطور الجريمة وتنوع أساليب ارتكابها وتعدد صفاتها خاصة جرائم الانترنت وتقنية المعلومات، وإنما يمكن وضع أسس عامة أو أركان للجريمة من خلالها يمكن التعرف عليها أو تحديد السلوك الإجرامي المستحدث المكون للجريمة، فإذا ما توافر هذا السلوك أو

---

oros), 1985, j, p.18. & M. Chawki, Combattre LaCybercriminalite, Universite Lyon III, France, 2008, p. 42.

(١) المادة الأولي من قانون مكافحة جرائم تقنية المعلومات الكويتي.

(٢) المادة الأولي من نظام مكافحة جرائم المعلوماتية السعودي.

العناصر أو الأركان أصبح الفعل أو العمل المرتكب عملاً إجرامياً يستوجب العقاب، على أن تترك مهمة البحث في مدي توافر تلك العناصر أو الأسس أو الصفات السلوكية لاجتهاد قاضي الموضوع.

وإن كان الأمر يلزمنا بتبني تعريف لجرائم تقنية المعلومات فنحن من جانبنا وبعد العرض لكل ما قيل في هذا الشأن من تعريفات يمكننا أن نعرف الجريمة التقنية بأنها كل فعل أو امتناع مجرم وغير مشروع يعاقب عليه القانون، يتم بواسطة شخص يتمتع بقدر من الذكاء الفني والتقنية العالية، ويقوم على مجموعة من العناصر المتداخلة التي تؤثر في طبيعة الأفعال الإجرامية المرتكبة سواء بشكل مباشر أو غير مباشر والمتصلة اتصالاً وثيقاً بالحاسب الآلي ووسائل التقنية الحديثة والتي لا يمكن بأي حال من الأحوال أن تتكون أو تنشأ أو يتصور وجودها من الأساس دون تحقق هذا الارتباط التقني بالحاسب الآلي .

وبهذا التعريف من وجهة نظرنا المتواضعة نكون قد جمعنا بين طياته كافة العناصر المكونة للجريمة، من حيث أن يكون هناك فعل أو امتناع غير مشروع يعاقب عليه القانون، فالفعل غير المجرم أو الغير معاقب عليه لا يعد جريمة لذا وضعت شرطا ليكون الفعل جريمة هو أن يكون منصوص على تجريمه وتفرض له عقوبة، وأن يكون مرتكب الجرم هو شخص فني عالي التقنية يتمتع بقدر من الذكاء، وأن تكون الوسيلة المستخدمة لارتكاب الجريمة هو الحاسب الآلي ذاته.

المطلب الثاني

الجهـود التشريعية المبذولة لمكافحة الجريمة التقنية

تمهيد:

تميزت طائفة الجرائم التقنية بتنوعها وظهورها بأشكال مختلفة ومعقدة، منها ما يمس حقوق ومصالح عامة للمجتمع، وما يمثل انتهاك لحقوق وحريات الأفراد، وأصبحت هذه الجرائم تشكل خطراً على الصعيدين الاقتصادي والقانوني، ناهيك عما تخلفه من تراجع وانهيار في مجال الاستثمار .

لذا كان من المتعين على المجتمع الدولي أن يتصدي لهذا الغزو الإجرامي التقني بسن المزيد من التشريعات والقوانين العقابية والإجرائية التي تتناسب وخطورة هذه الجرائم ووضع المزيد من الضوابط اللازمة لمواجهتها، وخلق آليّات قانونيّة للحماية من أخطارها، مع ضرورة أن تنصب هذه الجهود في عدة محاور منها تنظيم وحماية استخدام تقنية المعلومات من الجرائم والانتهاكات، حماية البيانات المتصلة بالحياة الخاصة، حماية حق المؤلف على البرامج وقواعد البيانات، حماية البيئة التقنية ذاتها.

وفي سبيل تحقيق ذلك مرت العملية التشريعية في مجال مكافحة الجريمة التقنية بالعديد من الجهود المتطورة على المستويين الأوروبي والعربي، ووضع نصوص عقابية وإجرائية رادعة، وهو ما سنبينه من خلال التقسيم التالي.

تقسيم:

سوف نقوم بتقسيم هذا المطلب الي فرعين كما يلي:

الفرع الأول: الجهــود التشريعية الأوروبيــة .

الفرع الثانى: الجهــود التشريعيــة العربيــة .

الفـرع الأول

الجهـود التشريعيـة الأوروبيـة

لقد اهتم المجتمع الدولي الأوروبي والأجنبي بتنظيم مجال تقنية المعلومات وبذل العديد من الجهود التشريعية من أجل التصدي لظاهرت الإجرام المعلوماتى، وكان من بين هذه الجهود ما قامت به الدول الآتية تباعاً[1]:

– **دولة السويد:** حيث أصدرت عام ١٩٧٣ أول قانون لها في مجال مكافحة تقنية المعلومات وهو قانون البيانات السويدي والذي اهتم بمعالجة قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، وهي بذلك تعتبر أول دولة تقوم فعلياً بإصدار تشريعات تتعلق بجرائم التقنية، لاسيما التزوير المعلوماتى.

– **دولة الدنمارك:** والتي لحقت السويد في هذا التطور الحاصل في مجال تقنية المعلومات بإصدارها أول قانون لها يتعلق بمكافحة جرائم الحاسب الآلي والانترنت عام ١٩٨٥، وكان من أهم نصوص هذا القانون ما تضمن منها فقرات خاصة بتحديد العقوبات والأفعال المجرمة التي تعد انتهاكاً للحاسب الآلي كالتزوير المعلوماتى .

– **بريطانيا:** بإصدارها لقانون مكافحة التزوير والتزييف عام ١٩٨٦م، وعرف أداة التزوير بأنها عبارة عن وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى .

---

(١) يراجع في ذلك: د/ ربيع محمود الصغير– القصد الجنائي– دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٥، ص٩٦، هامش ٣. ويراجع في ذلك أيضاً: ورقة بحثية بعنوان دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول– إدارة الدراسات والبحوث– مقدمة ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة الفترة من ٢٣– ٩/٢٥ الموافق ٧– ١٤٣٣/١١/٩هـ، ص١١ وما بعدها.

– **ألمانيا:** أصدرت عام ١٩٨٦م قانون خاص لمكافحة التزوير المعلوماتى والذي بموجه تكون لحقت عجلة التطور التشريعي الحاصل في مجال تقنية المعلومات.

– **فرنسا:** أصدرت القانون الفرنسي رقم ١٩ لسنة ١٩٨٨م الخاص بالتصدي للتزوير المعلوماتى .

– **الولايات المتحدة الأمريكية :** أصدرت العديد من التشريعات المتعلقة مجال تقنية وتكنولوجيا المعلومات، وكان من بينها القانون رقم ٤٧٤-٩٩-١٠٠ وهو قانون تشريعي عام شمل القانون التشريعي رقم ١٢١٣ لسنة ١٩٨٦ والمعدل للقانون (1030 s, s, u 18) الخاص بمواجهة جرائم الحاسوب.

– ولم يقف الأمر عند هذا الحد بل لقد أجتمع المجلس الأوروبي عام ٢٠٠١ في العاصمة المجرية بودابست في ٢٣ نوفمبر ٢٠٠١، للتشاور حول هذه الظاهرة الإجرامية المستحدثة والاتفاق على بنود واضحة لمكافحة هذه جرائم تقنية المعلومات، وقد أبرمت الاتفاقية الأوروبية الدولية لمكافحة الإجرام السيبيري (الإجرام عبر الانترنت)، ووقعت عليها٣٠ دولة، ثم انضم إليها العديد من الدول من خارج المجلس الأوروبي، وكان من أبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في ٢٢ سبتمبر ٢٠٠٦، ودخلت حيز النفاذ في الأول من يناير ٢٠٠٧، واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

الفـرع الثاني

الجهـود التشريعيـة العربيـــة

وعلى الجانب التشريعي العربي فهناك العديد من الدول العربية التي واكبت هذا التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على محاولة التصدي لمكافحة الجرائم الالكترونية الناشئة عنه بإصدارها عدد من التشريعات الخاصة، ومن بين هذه الدول ما يلي:

– **سلطنة عمان:** أصدرت عام ٢٠٠١ جملة من التشريعات لمكافحة الجريمة المعلوماتية تحت مسمى قانون مكافحة جرائم الحاسب الآلي (قانون مكافحة الجرائم الالكترونية)، وكان من أهمها الأتي:

المرسوم السلطاني رقم ٧٢ لسنة٢٠٠١م الصادر بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر) وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني تحت عنوان (جرائم الحاسب الآلي).

كما أنه تم إضافة مواد إلى قانون الاتصالات العماني تحرم تبادل الرسائل التي تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد، ثم ووضعت السلطنة قانوناً ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة.

– **دولة المغرب**: سعي المشرع المغربي لوضع نصوص تشريعية تعمل على تنظيم المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي عن طريق إدخاله لبعض الفصول التشريعية التي تعاقب على الأفعال التي تشكل جرائم تحت عنوان (المس بنظام المعالجة الآلية للمعطيات) وذلك بموجب القانون رقم ٠٧.٠٠٣ الصادر بتاريخ ١٦ رمضان ١٤٢٤ الموافق ١١ نوفمبر ٢٠٠٣.

- **دولة الإمارات العربية المتحدة:** لقد كان اهتمام دولة الإمارات العربية بمكافحة الجريمة المعلوماتية والتصدي لأخطارها اهتماماً واضحاً، حيث أصدرت العديد من التشريعات المتعلق بهذه النوعية من الجرائم المعلوماتية عالية التقنية من بينها :

القانون العربي الاسترشادي الصادر عام ٢٠٠٣ بشأن مكافحة جرائم تقنية المعلومات وما في حكمها، المعتمد بموجب قرار مجلس وزراء العدل العرب المنعقد في دورته التاسعة عشرة رقم (٤٩٥ - د١٩- ٢٠٠٣/١٠/٨) ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (٤١٧- د٢١/٢٠٠٤).

وفي عام ٢٠٠٦ أصدرت القانون رقم ٢ لسنة ٢٠٠٦ الخاص بمكافحة جرائم تقنية المعلومات، ثم تلاه إصدار القانون رقم ٣ لسنة ٢٠١٢ الخاص بإنشاء الهيئة الوطنية للأمن الالكتروني، وفي عام ٢٠١٢ أصدرت المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ المتعلق بمكافحة جرائم تقنية المعلومات، وفي عام ٢٠١٨ قامت بإصدار المرسوم الاتحادي رقم ٢ لسنة ٢٠١٨، الخاص بتعديل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢.

وبذلك تعتبر دولة الإمارات أول دولة عربية تقوم بإصدار تشريع قانوني مستقل يتعلق بمكافحة الجرائم المعلوماتية هو القانون رقم ٢ لسنة ٢٠٠٦.

- **المملكة العربية السعودية:** حيث أصدرت عام ٢٠٠٧ أولي قوانينها في مجال المكافحة التشريعية لجرائم تقنية المعلومات تحت عنوان نظام مكافحة الجرائم المعلوماتية، وأقره مجلس الوزراء بالقرار رقم ٧٩ بتاريخ ١٤٢٨/٣/٧هـ، وتم التصديق عليه بالمرسوم الملكي رقم ١٧م بتاريخ ١٤٢٨/٣/٨هـ، وصدر بالقرار رقم ١١٥٦٧/ب- بتاريخ ١٤٢٨/٣/٩هـ، وكان الهدف منه الحد من نشوء هذه الجرائم المعلوماتية، فقد جاء في المادة الثانية من هذا النظام:(يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد

هذه الجرائم والعقوبات المقررة لكل منها، بما يؤدي إلى ما يلي: (١- المساعدة على تحقيق الأمن المعلوماتى. ٢- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية. ٣- حماية المصلحة العامة، والأخلاق، والآداب العامة. ٤- حماية الاقتصاد الوطني).

- **دولة الكـــويت:** نظمت دولة الكويت استخدام وسائل التقنية الحديثة وتجريم الانتهاكات التي تحدث منها أو عليها بإصدار حزمة من التشريعات كان من بينها: (القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية، والقانون رقم ٩ لسنة ٢٠٠١ بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت والقوانين المعدلة له، القانون رقم ٣ لسنة ٢٠٠٦ بشأن المطبوعات والنشر، القانون رقم ٦١ لسنة ٢٠٠٧ بشأن الإعلام المرئي والمسموع، القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية، القانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة ٢٠١٥).

جمهورية مصر العربية: لقد كان حرص المشرع المصري عظيماً في مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العالم في العصر الحديث، بإصداره العديد من التشريعات اللازمة لمواجهة هذا الغزو التقني ودخول الرقمية فضائها المعلوماتى، ومن هذه التشريعات قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣م الخاص بتأمين نقل وتبادل المعلومات[١]، والقانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"[٢]، القانون رقم

---

(١) وعرفت المادة الأولي من هذا القانون وسائل الاتصالات بأنها: (أية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أياً كانت طبيعتها، وسواء كان الاتصال سلكياً أو لاسلكيًا)، وقد اقر المشرع في الباب السابع من هذا القانون مجموعة من العقوبات التي تطبق إزاء التعرض أو الاعتداد على تلك الخدمات أو استغلالها بطرق غير مشروعة.

(٢) راجع: القرار بقانون رقم ١٥ لسنة ٢٠٠٤ الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ لسنة ٢٠٠٥-

١٤٣ لسنة ١٩٩٤ بشأن الأحوال المدنية، والدستور المصري لعام ٢٠١٤ والذي تضمن العديد من المواد التي تهدف إلى إقرار حماية خاصة لمختلف نواحي التعاملات التقنية والرقمية وتنظيمها(١).

هذا إلى جانب العديد من القرارات التنظيمية التي أصدرتها الوزارة المعنية بتكنولوجيا المعلومات والاتصالات بهدف حماية تقنية المعلومات والاتصالات(٢)، ومازال هناك العديد من الدراسات القانونية والجهود التشريعية التي تبذل من أجل تأمين المعاملات الالكترونية المختلفة من كافة جوانبها القانونية والجنائية.

وقد أنشأت مصر بموجب قرار مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ مجلس أعلي للأمن السيبرانى(٣)، لتكون مهمته وضع إستراتيجية وطنية لمواجهة

بشأن إصدار اللائحة التنفيذية لقانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

(١) حيث نصت المادة ٣١ من الدستور المصري لعام ٢٠١٤ على أن " أمن الفضاء المعلوماتى جزء من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليها، على النحو الذي ينظمه القانون". كما تنص المادة ٥٧ من ذات الدستور على أن " للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمه، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك"

(٢) **من بين هذه الجهود والمحاولات التشريعية الأخرى ما يلي:** " قرار وزير الاتصالات ١٠٧ لسنة ٢٠٠٥ بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات.، قرار وزير الاتصالات ١٢٨ لسنة ٢٠٠٦ بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات، وإنشاء إدارة تسمى (إدارة فض المنازعات) بالجهاز.، قرار وزير الاتصالات رقم ١٠٨ لسنة ٢٠٠٥ بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات.

(٣) نشر هذا القرار بالجريدة الرسمية في ديسمبر ٢٠١٤، العدد الخمسون، بتاريخ ٢٠١٤/١٢/١٥. وتضمن على أن ينشأ مجلس أعلي لأمن البنية التحتية للاتصالات وتكنولوجيا المعلومات يتبع رئاسة مجلس الوزراء ويسمي المجلس الأعلى للأمن السيبراني، ويشكل برئاسة وزير الاتصالات وتكنولوجيا المعلومات وعضوية ممثلي وزارات: (الدفاع، الخارجية، الداخلية، البترول، الثروة المعدنية، الكهرباء والطاقة المتجددة، والصحة والسكان، الموارد المائية والري، والتموين والتجارة الداخلية، الاتصالات

الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها تمشياً مع التطورات التقنية، وبتاريخ ٢٠١٤/٩/١٩ أصدر السيد رئيس الجمهورية القرار رقم ٢٧٧ لسنة ٢٠١٤[١]، بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١.

وكان أخر هذه التطورات التشريعية وأهمها القانون رقم ٢٠١٨/١٧٥ الصادر بشأن مكافحة جرائم تقنية المعلومات[٢] ولائحته التنفيذية رقم ٢٠٢٠/١٦٩٩[٣].

– **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** الموقعة في القاهرة بتاريخ ٢١ ديسمبر٢٠١٠، ووافقت مصر على الانضمام إليها بموجب قرار رئيس الجمهورية رقم ٢٧٦ لسنة ٢٠١٤ بتاريخ ١٩ أغسطس ٢٠١٤ والمنشور بالجريدة الرسمية بالعدد ٤٦ في ١٣ نوفمبر ٢٠١٤، وذلك مع التحفظ على شرط التصديق، وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

وتعد هذه الاتفاقية من أهم الاتفاقيات العربية التي أبرمت في مجال مكافحة الجريمة التقنية بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، مثل الاعتداء على سلامة البيانات، وجرائم إساءة استخدام وسائل تقنية المعلوماتية، والتزوير والاحتيال والإباحية والاعتداء على حرمة الحياة الخاصة، والجرائم المتعلقة

وتكنولوجيا المعلومات) وجهاز المخابرات العامة، والبنك المركزي المصري، وعدد ٣ من ذوي الخبرة في الجهات البحثية والقطاع الخاص يرشحهم المجلس، ويصدر بتعيينهم قرار من وزير الاتصالات وتكنولوجيا المعلومات.

(١) منشور بالجريدة الرسمية، العدد٤٧، بتاريخ ٢٠/ نوفمبر ٢٠١٤.

(٢) منشور بالجريدة الرسمية – العدد ٣٢ مكرر (ج) بتاريخ ٢٠١٨/٨/١٤.

(٣)المنشور بالجريدة الرسمية في العدد ٣٥ تابع (ج) – بتاريخ ٢٧ أغسطس سنة ٢٠٢٠.

بالإرهاب والمرتكبة بواسطة تقنية المعلومات مثل نشر أفكار جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية ونشر طرق صناعة المتفجرات، وأيضا ما يتعلق بالجريمة المنظمة مثل غسل الأموال والترويج للمخدرات والاتجار بالبشر والأعضاء البشرية والأسلحة .

وكان ذلك عرض سريع لأهم التطورات التشريعية التي حدثت على المستويين العالمي والإقليمي في مجال مكافحة الجريمة التقنية، ولكن ما يهمنا هنا هو ما صدر مؤخراً من تشريعات عربية في هذا الشأن، وعرض لما جانبها من صواب أو شابها من عيوب وانتقادات، وهو ما سوف تنصب عليه دراستنا الماثلة تباعاً .

المطلب الثالث

ضوابط التعاون الدولي وتحديد الاختصاص القضائي

تمهيد:

لقد أثارت الجرائم المعلوماتية العديد من المشكلات نظراً لطبيعتها الخاصة وما تمتاز به من تعقيد وسرعة في ارتكابها إلى جانب قدرة الجناة على الهرب والتخفي، إضافة إلى كونها جرائم عابرة للحدود والقارات، فقد ترتكب هذه الجرائم داخل النطاق الإقليمي لإحدى الدول وتتحقق نتائجها خارج هذا النطاق أي داخل دولة أخري، مما أثار ذلك إشكالية غاية في الأهمية والتعقيد تتمثل في تحديد الاختصاص القانوني والقضائي لهذه الجرائم المستحدثة، ودور التعاون الدولي في مجال مكافحة هذه الجريمة، وهو ما سنتناوله تفصيلاً من خلال التقسيم التالي.

تقسيم:

سوف نقوم بتقسيم دراسة هذا المطلب إلى فرعين على النحو التالي:

الفرع الأول: ضوابط التعاون الدولي في مجال مكافحة الجريمة.

الفرع الثاني: النطاق المكاني للقانون وتحديد الاختصاص القضائي .

الفرع الأول

ضوابط التعاون الدولي في مجال مكافحة الجريمة

لقد كان حرص المشرع المصري واهتمامه واضحاً في تيسير سبل التعاون الدولي في مجال مكافحة الجريمة قبل وقوعها، وتبادل المعلومات والبيانات اللازمة عنها حال وقوعها، وضبط وتسليم المجرمين الهاربين، والمساعدة في إجراء التحقيق معهم، أي تطبيق مبدأ العالمية الجنائية والإجرائية، وقواعد تسليم المجرمين الهاربين في إطار الاتفاقيات والمعاهدات الدولية والإقليمية المصدق عليها فيما بينهم، وظهر ذلك بوضوح في المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات المصري التي نصت على أن" تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقاً لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن"(١).

ويعد مسلك المشرع المصري بإدراج نص خاص يتضمن الاهتمام بالتعاون الدولي وتيسيره في مجال مكافحة الجريمة المعلوماتية التقنية تفعيلاً حقيقياً لمبادئ وأهداف الاتفاقية العربية لمكافحة الجريمة المعلوماتية، الواردة في المادة الأولي منها والتي نصت على أن تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

والى جانب هذا الهدف الرئيسي والهام فقد تضمنت الاتفاقية العربية العديد من النصوص المتعلق بتفعيل التعاون الدولي في مجال مكافحة هذه الطائفة من

---

(١) المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات المصري.

الجرائم المستحدثة، بدءا من المادة ٣٠ وحتى المادة ٤٣ من الاتفاقية[١] .

أما على جانب التشريعات المقارنة، فقد تلاحظ لنا أنها قد سلكت مسلكاً مغايراً لما اتخذه المشرع المصري، فإذ البين أن نصوص وتشريعات كل من الكويت والإمارات والسعودية لم يحالفها التوفيق وأصابها القصور لإغفالها مثل هذا الاتجاه التشريعي، وعدم تضمين نصوصها ما يفيد الاهتمام بالتعاون الدولي في التصدي لهذه الظاهرة الإجرامية أو النص على توجيه المجتمع المحلي والدولي بمثل هذا التعاون رغم أهميته بالنظر لطبيعة مثل هذه الجرائم التقنية والتي تتميز بكونها جرائم عابرة للحدود والقارات وتتطلب مزيد من التنظيم والتعاون الدولي فيما بين جميع الدول.

الفرع الثاني

النطاق المكاني للقانون وتحديد الاختصاص القضائي

الأصل في تطبيق نصوص قانون العقوبات هو مبدأ الإقليمية ويقصد بهذا المبدأ أن قانون العقوبات يطبق علي كل جريمة ترتكب في إقليم الدولة، سواء أكان الجاني وطنيا أم أجنبيا، وسواء أكان المجني عليه فيها وطنيا أم أجنبيا . ويرجع السبب في إعمال مبدأ الإقليمية إلى الطبيعة الخاصة لقانون العقوبات، باعتباره معبراً عن سيادة الدولة، فإذا ما وقعت الجريمة على إقليم الدولة فإن قانون العقوبات يصبح واجب التطبيق، كما يصبح القضاء الوطني مختصا بمحاكمة المتهم بغض النظر عن جنسيته أو ديانته.

إلا أن المشرع في قانون مكافحة جرائم تقنية المعلومات تبني مبدءاً مغايراً لما هو متبع وهو مبدأ العينية وجعل أحكام ونصوص هذا القانون تسري علي الجرائم المرتكبة حتى ولو خارج الإقليم المصري من غير المصريين متى كان معاقبا علي ذات الفعل في قانون الدولة التي ارتكب على أرضها تحت أي وصف، فيُقصد بمبدأ العينية سريان قانون العقوبات على جرائم معينة تقع في

(١) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة البيان.

خارج البلاد بغض النظر عن جنسية الفاعل في تلك الجرائم بسبب تعلقها بمصالح جوهرية للدولة.

ليس ذلك فحسب بل أخذ هذا القانون الحديث بتطبيق مبدأ العالمية الجنائية[١] ولكن بشكل مقيد أي سريان أحكام هذا القانون على هذه الجرائم التي تتعلق بتقنية المعلومات والتي تقع خارج البلاد حتى وإن كان الفاعل غير مصري وهو ما يسمي بالاختصاص السلبي[٢] الذي يسمح للدولة بالمتابعة الجنائية ضد مرتكبي الجرائم على أساس جنسية المجني عليهم[٣].

والجدير بالذكر أن البحث في النطاق المكاني لتطبيق قانون مكافحة جرائم التقنية المعلوماتية من أهم وابرز الأمور التي نظمها المشرع المصري، وحرص على النص عليها صراحة وإدراجها ضمن نصوص قانون مكافحة جرائم تقنية المعلومات، وتبني مبدأ العينية بدلاً من الإقليمية وبالتالي إسناد مهمة الاختصاص القضائي للقاضي الوطني حتى وإن كان لم يرد النص على هذا الاختصاص صراحة، فهو أمر يفهم ضمناً من نص المادة الثالثة الواردة بقانون مكافحة جرائم تقنية المعلومات والتي تضمنت النص على تحديد النطاق المكان لتطبيق القانون، حيث نصت المادة الثالثة من هذا القانون على أنه [٤]: " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني".

---

(١) د/ مروي السيد الحصاوي– مبدأ العالمية في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠١٩، ص١٠٢.

(٢) د/ سليمان عبد المنعم– النظرية العامة لقانون العقوبات– دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠، ص١٢٧.

(٣) د/ أحمد شوقي عمر أبو خطوة– شرح الأحكام العامة لقانون العقوبات، الجزء الأول– النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ١٩٩٩، ص١١٧.

(٤) يراجع نص المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات المصري.

هذا وقد تناولت تلك المادة تحديد حالات تطبيق القانون من حيث المكان على الجرائم المعلوماتية التي ترتكب خارج حدود الدولة المصرية وبالتالي منح الاختصاص القضائي للقاضي الجنائي الوطني على النحو التالي:

١- إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

٢- إذا كان المجني عليهم أو أحدهم مصرياً.

٣- إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في مصر.

٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها مصر.

٥- إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج.

٦- إذا وُجد مرتكب الجريمة في مصر، بعد ارتكابها ولم يتم تسليمه.

وقد أحسن المشرع المصري صنعاً بتبنيه هذا الاتجاه المتمثل في تحديد النطاق المكاني لتطبيق أحكام القانون وبيان حدود سريانه سواء من حيث الجناة أو المجني عليهم، ومن ثم تحديد القاضي الجنائي المختص بهذه الجرائم وهو ما يتفق مع ما ورد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي نصت في المادة ٣٠ من الفصل الرابع منها على أن:

١- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: (أ- في إقليم الدولة الطرف. ب- على

متن سفينة تحمل علم الدولة الطرف. جـــ- على متن طائرة مسجلة تحت قوانين الدولة الطرف. د-من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. هـــ – إذا كانت الجريمة تمس أحد المصالح العليا للدولة).

٢- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (١) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

- **أما في مجال التنازع القضائي**، سواء تعلق الأمر بتنازع قضائي دولي أو تنازع قضائي محلي، وهو ما سنتناوله على النحو التالي:

أولاً: بالنسبة للتنازع القضائي المحلي: فقد أسند المشرع في المادة (٤) من القانون ١٢٠ لسنة ٢٠٠٨ الصادر بإنشاء المحاكم الاقتصادية وتعديلاته مهمة الفصل في النزاعات وجرائم الجنح التي ترتكب نتيجة تطبيق أحكام هذا القانون للمحكمة الاقتصادية بدوائرها المختلفة، حيث نصت هذه المادة على أن " تختص الدوائر الابتدائية والاستئنافية بالمحاكم الاقتصادية ، دون غيرها ، نوعيا ومكانيا بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها فى القوانين الآتية: "..٩-قانون حماية حقوق الملكية الفكرية. ١٦-قانون تنظيم الاتصالات.١٧-قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات."

ولما كانت جرائم التقنية المعلوماتية الواردة بالقانون رقم ١٧٥ لسنة ٢٠١٨ تتشابه إلى حد كبير من حيث الطبيعة والصفات والأساليب مع ذات الجرائم المشار إليها في المادة رقم (٤) سالفة البيان، الأمر الذي يؤكد تفرد واستقلال المحكمة الاقتصادية بدوائرها المختلفة بنظر الفصل في الجرائم والنزاعات التي تنشأ نتيجة تطبيق أحكام هذا القانون رقم ١٧٥ لسنة ٢٠١٨ فيما يتعلق بمكافحة

جرائم تقنية المعلومات، وبذلك فهي ليست بحاجه إلى النص صراحة على ذلك[١].

ثانياً: وبالنسبة للتنازع القضائي الدولي: فقد اهتمت الاتفاقية العربية بمسألة تحديد القاضي الجنائي المختص بنظر الجرائم المعلوماتية المرتكبة بواسطة وسائل التقنية الحديثة اهتماماً ملحوظاً، وعملت على وضع الحلول للنزاعات التي قد تنشأ بشأن التنازع القضائي سواء أكان هذا التنازع تنازعاً ايجابياً بادعاء أكثر من دولة باختصاصها القضائي بنظر جريمة تقنية وتمسكها بذلك الادعاء، أو تنازع سلبي وهو تخلي وإنكار للدول عن اختصاصها القضائي وقامت بتحديد القاضي المختص وفقاً لدرجة الخطورة أو الضرر الواقع على الدولة ودرجة المساهمة الإجرامية، ووضعت شرطاً لتفعيل ذلك وهو ضرورة أن تكون هذه الدولة طرفاً في الاتفاقية العربية المبرمة، على النحو التالي[٢]:

حيث جعلت هذه الاتفاقية قاضي الدولة التي أخلت الجريمة بأمنها ومصالحها وتسببت في الإضرار بها في مقدمة القضاة المختصين ليكون هو صاحب الاختصاص الأصيل وفي المرتبة الأولي وأولي من غيره في تبني إجراءات المحاكمة والعقاب، ثم يأتي في المرتبة التالية من حيث الأهمية والاختصاص قاضي الدولة التي وقعت الجريمة على إقليمها حتى وإن لم ينتج عنها ضرر أو تهديد أمني لهذه الدولة، ثم يكون الاختصاص لقاضي الدولة التي ينتمي إليها الجاني أو الجناة أي لقاضي الدولة التي يكون الشخص المطلوب من رعاياها، وتقول هذه الاتفاقية أنه في جميع الأحوال إن اتحدت الظروف المشار إليها يكون الاختصاص لقاضي الدولة الأسبق في تقديم طلب التسليم للمحاكمة .

---

(١) وهو ذات ما تبنته محكمة النقض المصرية في حكمها الصادر في الطعن رقم ٧٨٤٣ لسنة ٨٧ ق– جلسة ٢٠١٩/١/٢٠.

(٢) تنص الفقرة الثالثة من المادة ٣٠ من الاتفاقية العربية لمكافحة الجريمة المعلوماتية، على أن " .... ٣– إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم ".

وعلى الرغم من أهمية هذه الإشكالية المتمثلة في تنازع الاختصاص القضائي، إلا أننا لم نرى لها صدي لدي المشرع المصري، حيث لم يرد النص عليها بشكل صريح ضمن أحكام ونصوص قانون جرائم التقنية المعلوماتية، لذا نري ضرورة إجراء تعديل لنصوص هذا القانون لكي يتضمن النص صراحة على تنظيم وتحديد القاضي المختص بنظر هذه الطائفة من الجرائم المعلوماتية، ونوصي المشرع المصري بضرورة تبني الاتجاه الوارد بالاتفاقية العربية لمكافحة جرائم التقنية سالف البيان .

المبحث الثاني

أنماط الجرائم وحدود العقوبات المقررة لها

تمهيد:

إضافة لما قدمته وسائل التقنية الحديثة من مزايا ومساعدات عديدة للإنسانية جمعاء لمواجهة التطورات والاحتياجات الحياتية، خلفت أيضاً العديد من المساوئ والسلبيات الضارة، حيث استخدمها المجرمون في تحقيق أهدافهم غير المشروعة فكانت أداة جديدة غيرت من شكل الجريمة بصفة عامة سواء كانت أداة لارتكابها أو مسرحاً لها، وهو ما أطلق عليه– الإجرام الحديث Modern Crim، أو الإجرام التقني Technical Crim، الذي أفرز نوعية جديدة من الجرائم سميت بجرائم التقنية، أو جرائم المعلوماتية ارتباطاً بشبكة المعلومات الدولية(١).

والجدير بالذكر أن المشرع المصري تناول تحديد هذه النوعية من الجرائم في الباب الثالث من قانون مكافحة جرائم تقنية المعلومات، وأفرد لكل منها عقوبة خاصة بها تتناسب وجسامة الجرم المرتكب ومدي خطورته وإضراره بالأفراد والمجتمع، أي تحديد العقوبات الكفيلة بمكافحة هذه النوعية من الجرائم المستحدثة ومعاقبة مرتكبيها، وتتأرجح هذه العقوبات مابين التخفيف والتشديد حسب الخطورة الإجرامية وحجم الأضرار المترتبة عليها، هذا وقد نص المشرع على ضرورة الأخذ في الاعتبار عند تطبيق هذه العقوبات عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، ومع مراعاة أحكام قانون

(1)Melanie Kowalski, «Cybercriminalité, enjeux, sources de données et faisabilité de recueillir des données auprès de la police», Centre canadien de la statistique juridique, catalogue No 85-558-XIF, Décembre 2002, visible:
http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85-558-XIF2002001.pdf.

الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦ [١].

وفي ضوء ذلك سوف نتناول أهم هذه الجرائم والعقوبات المقررة لها وفقاً لأحكام قانون مكافحة جرائم تقنية المعلومات في مصر والدول المقارنة، من خلال تقسيم الدراسة فى هذا المطلب على النحو التالي.

تقسيم:

سوف نقوم بتقسيم هذا المبحث إلى ثلاث مطالب على النحو التالي:

المطلب الأول: جرائم الشبكات وأنظمة وتقنيات المعلومات.

المطلب الثاني: الجرائم المتعلقة بالبريد الالكتروني والمواقع أو الحسابات الخاصة.

المطلب الثالث: جرائم الاعتداء على حرمة الحياة الخاصة وانتهاك الخصوصية.

(١) تنص المادة ١٢ من قانون التقنية المعلومات المصري على أنه: " مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، ومع مراعاة أحكام قانون الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦، يعاقب على الجرائم التالية بالعقوبات المبينة قرين كل جريمة ".

المطلب الأول

جرائم الشبكات وأنظمة وتقنيات المعلومات

تمهيد:

لقد تعددت هذه النوعية من الانتهاكات والجرائم التقنية وصنفها المشرع المصري إلى طوائف عدة بحسب طبيعتها وأسلوب ارتكابها، فمنها جرائم الدخول والانتفاع غير المشروع بالخدمات التقنية، وجرائم الاعتداء على سلامة البيانات والنظم المعلوماتية، وجرائم الحيازة والاتجار بوسائل التقنية، والجرائم المرتكبة من مدير الموقع، وسوف نتناول هذه الطائفة من الجرائم من خلال التقسيم التالي.

تقسيم:

سوف نقوم بتقسيم دراسة هذا المطلب الى ثلاثة فروع كما يلي:

الفرع الأول: جرائم الدخول والانتفاع غير المشروع.

الفرع الثاني: جرائم الاعتداء على البيانات والنظم المعلوماتية.

الفرع الثالث: جرائم الاحتيال المالي والحيازة والاتجار غير المشروع بوسائل تقنية المعلومات.

الفرع الأول

جرائم الدخول والانتفاع غير المشروع

لقد استخدمت تقنية المعلومات على نطاق واسع في كافة المجالات الحياتية، وتم الاعتماد عليها في تسيير أمور وشئون المجتمع ككل لتحل تدريجياً محل الأيدي العاملة، وصاحب ذلك قيام بعض الجهات أو الأشخاص بمحاولة الدخول إليها واستغلالها والانتفاع بها دون وجه حق أو بمقابل مشروع، فتدخل المشرع لحماية هذه الوسائل التقنية من مثل هذه الجرائم ومنع استغلالها بطرق غير المشروعة، كما يلي:

أولاً: جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها:

يقصد بالانتفاع هو تحقيق قدر معين من الاستفادة سواء أكانت استفادة مادية أو معنوية أو أدبية، وقد اعتبر المشرع المصري أن هذا الانتفاع أو الاستغلال واستخدام هذه التقنية دون حق مشروع من قبيل الأفعال غير المشروعة المجرمة أو القرصنة التي تستوجب العقاب، بل اعتبرها جريمة تشبه إلى حد كبير جريمة السرقة، وعرفها في المادة ١٣ من قانون مكافحة تقنية المعلومات بأنها كل انتفاع يتم بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي(١).

وقد نهج المشرع الإماراتي ذات نهج المشرع المصري بتجريم فعل الانتفاع دون وجه حق في المادة ٣٤ من قانون المكافحة التقنية الإماراتي، ولكنه لم يقصرها على مجرد الانتفاع الفردي فقط، بل أضاف إليها فعل تجريمي أخر وهو

---

(١) تنص المادة ١٣ من القانون المصري على أن " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي".

تسهيل الانتفاع للغير، وأفرد لها بذات المادة عقوبة أكثر تشدداً عما أورده المشرع المصري[١].

أما على الجانبين الكويتي والسعودي فلم يرد بهما أية نصوص تتطرق لمثل هذا الاتجاه التجريمي، كما لم يرد مثل هذا النص بنصوص الاتفاقية العربية لمكافحة الجريمة التقنية.

ثانياً: جريمة الدخول غير المشروع -Haching :

يقصد بالدخول غير المشروع أو الهكترة هو النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح[٢]. أو هو دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع اليكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية وغير مصرح لذلك الشخص بالدخول إليها[٣].

ولم يرد بقانون تقنية المعلومات المصري تعريف واضح ومحدد لفعل الدخول غير المشروع إلا أنه من الجائز استنباط هذا التعريف من نص المادة (١٤) منه بأنه كل دخول يحدث عمدا، أو بخطأ غير عمدي والبقاء بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه ".

وقد عاقب المشرع المصري على مجرد ارتكاب فعل الدخول غير المشروع إلى مواقع أو حسابات خاصة أو أنظمة تقنية المعلومات والبقاء بها دون وجه حق، سواء أكان هذا الدخول قد تم بعمد أو بدون عمد عن طريق الخطأ، وبشرط

---

(١) تنص المادة ٣٤ من التشريع الإماراتي على أن "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم، أو بإحدى هاتين العقوبتين كل من انتفع أو سهل للغير بغير وجه حق الانتفاع بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية، وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات".

(٢) المادة الأولي من قانون مكافحة جرائم تقنية المعلومات الكويتي.

(٣) المادة الأولي من نظام مكافحة جرائم المعلوماتية السعودي.

أن يكون هذا الدخول محظوراً[١]، أما وإن تسبب هذا الدخول غير المشروع في حدوث أضرار معلوماتية أو نتج عنه مخاطر تتمثل في إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، فهنا الوضع يختلف تماماً، حيث شدد المشرع المصري وضاعف من حد العقوبة المقررة له[٢].

ويكمن الهدف من وراء هذا التجريم في حماية الأنظمة والبرامج المعلوماتية من عمليات التطفل والقرصنة عن طريق ما يعرف بالدخول غير المشروع سواء أكان الدخول في جزء من النظام أو في جميع أجزاءه أو في كافة الأنظمة التقنية .

وقد سلك المشرع الكويتي في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات ذات مسلك المشرع المصري بتجريم ذات الأفعال، وضاعف من حد العقوبة المقررة لهذه الأفعال إذا ما اقترنت جريمة الدخول غير المشروع بحالات أخري تستوجب التشديد نظراً لخطورتها وجاء ذلك في المادتين الثانية[٣] والثالثة[٤] من ذات التقنيين.

كما ذهب المشرع الإماراتي إلي تجريم فعل الدخول غير المشروع إلى موقع أو نظام أو شبكة معلوماتية أو أية وسيلة تقنية معلومات، طالما تم ذلك دون تصريح أو تجاوز المصرح له حدود هذا التصريح، ولم يقف الأمر عند ذلك الحد

---

(١) تنص الفقرة الأولي من المادة ١٤ من قانون مكافحة جرائم تقنية المعلومات المصري على أن "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

(٢) تنص الفقرة الثانية من المادة ١٤ من قانون التقنية المصري على أن " فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين ".

(٣) يراجع نص المادة الثانية من قانون المكافحة التقنية الكويتي سالف البيان.

(٤) يراجع نص المادة الثالثة من قانون المكافحة التقنية الكويتي سالف البيان.

فقط بل توسع المشرع الإماراتي وأدرج ضمن هذه الأفعال فعل البقاء في هذه الأنظمة أو الشبكات بصورة غير مشروعة حتى وإن كان الدخول الأول قد تم بطريقة مشروعة[١].

والجدير بالذكر أن المشرع الإماراتي كان حريصاً على متابعة كل تطور ووضع بين نصب عينيه ما اتبعه المشرع الكويتي وسار على خطاه في تشديد العقوبة المقضي بها إذا ما اقترن فعل الدخول بأفعال أخري تزيد من خطورة الفعل المرتكب[٢] .

وهو ذات ما تبناه المشرع السعودي في الفقرتين (٢، ٣) من المادة الثالثة[٣]، خاصة وأنه قد حرص على مضاعفة حد العقوبة المقررة إذا كان فعل الدخول غير المشروع مقروناً بأي من الأفعال الضارة الآتية:

١- الوصول- دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات[٤].

٢- إذا كان الدخول بهدف إلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو

---

(١) راجع نص الفقرة الأولي من المادة الثانية من قانون مكافحة جرائم المعلوماتية الإماراتي.

(٢) مشار إلي هذه الأفعال في المواد الثانية، والثالثة، والرابعة، والخامسة من التقنين الإماراتي سالف البيان.

(٣) تنص المادة الثالثة من نظام المكافحة السعودي على أن" يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: "١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي- دون مسوغ نظامي صحيح- أو التقاطه أو اعتراضه. ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً. ٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه. ٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها. ٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة" .

(٤) راجع نص الفقرة الثانية من المادة الرابعة من نظام المكافحة السعودي .

تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها[١].

٣- إذا كان الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني[٢].

وفي جميع الأحوال نص المشرع السعودي على ضرورة أن لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية[٣] :

- ارتكاب الجاني الجريمة من خلال عصابة منظمة.
- شغل الجاني لوظيفة عامة، واتصلت الجريمة بهذه الوظيفة، أو كان ارتكابه للجريمة من خلال استغلاله لسلطاته أو نفوذه الوظيفية.
- التغرير بالقُصر ومن في حكمهم، واستغلالهم.
- إذا كانت هناك أحكام محلية أو أجنبية سابقة بالإدانة صدرت بحق الجاني في جرائم مماثلة .

ونخلص من هذا العرض المبسط لجريمة الدخول غير المشروع في ضوء أحكام التشريع المصري مقارناً ببعض التشريعات العربية أن جميع هذه التشريعات تتفق فيما بينها في العديد من الجوانب والنصوص التشريعية، مع وجود بعض الأوجه الخلافية الضئيلة التي لا تؤثر على الجوانب الاتفاقية منها، ومن هذه النواحي الخلافية الآتية :

١- أن كل من المشرع الكويتي والسعودي لم يتطرقا إلى فعل البقاء المتعمد الذي يتحقق في حالة الدخول غير المشروع أو الدخول المشروع إلى أنظمة

---

(١) راجع نص الفقرة الأولي من المادة الخامسة من نظام المكافحة السعودي .

(٢) راجع نص الفقرة الثانية من المادة السابعة من نظام المكافحة السعودي .

(٣) راجع نص المادة الثامنة من نظام المكافحة السعودي .

التقنية المعلوماتية على الرغم من انتهاء الفترة المقررة لدخول الجاني والبقاء داخل النظام، على عكس ما اتبعه كل من المشرع المصري والإماراتي ووفقاً لما هو وارد في المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات(١).

٢- أن المشرع المصري جعل من فعل البقاء المتعمد في حالة الدخول المشروع وتجاوز هذا الحق في الدخول بالبقاء بعد فوات المواعيد جريمة مستقلة وأوردها في مادة مستقلة وقرر له عقوبة مغايرة اقل حدة وتشدد عن سابقتها من جريمة الدخول غير المشروع (٢).

٣- أن المشرع الكويتي توسع في ذكر وتعداد أوجه التعدي التي ترتكب من خلال فعل الدخول غير المشروع والتي اعتبرها جريمة في حد ذاتها تستوجب التشديد، وكان من بينها على سبيل المثال الآتي:

- ما ورد في الفقرة الثانية من المادة الثالثة التي تناولت تجريم فعل التزوير أو الإتلاف لمستند أو سجل أو توقيع اليكتروني يحدث نتيجة الدخول غير المشروع... إلى أخر الفقرة، وهو ذات ما أورده المشرع الإماراتي في المادة السادسة منه حينما نص على جريمة تزوير مستند حكومي أو غير حكومي، وضاعف من حد العقوبة في حالة استعمال هذا المستند مع علم الجاني بتزويره، مع اختلاف أن المشرع الإماراتي لم يقرنه بجريمة الدخول غير المشروع، فقرر لها عقوبة رادعة سواء ارتكبت من خلال دخول مشروع أو غير مشروع. وتشدد أكثر من ذلك في حالة إذا ما وقع هذا التزوير على مستند رسمي أو بنكي أو مستندات حكومية.

---

(١) تنص السادسة من الاتفاقية العربية على أن " جريمة الدخول غير المشروع :
١- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
٢- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: أ - محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. ب-الحصول على معلومات حكومية سرية.

(٢) راجع المادة ١٥ من قانون مكافحة جرائم تقنية المعلومات المصري .

– وفي الفقرة الأخيرة من المادة الثالثة نص المشرع الكويتي على جريمة النصب أو الاحتيال الالكتروني إذا ما تم الاستيلاء للنفس أو للغير – بطرق احتيالية أو اسم كاذب أو انتحال صفة – على مال أو منفعة أو مستند أو توقيع على مستند، من خلال شبكة المعلومات أو باستخدام وسيلة تقنية . وهو خلافاً لما اتبعه المشرع السعودي الذي تناول جريمة النصب أو الاحتيال الالكتروني في مادة مستقلة منه ولم يجعلها حالة من حالات تشديد العقوبة[١]، وهو ذات ما فعله المشرع الإماراتي في المادة الحادية عشر منه[٢]. وعلى العكس من ذلك فلم نجد لهذه الحالات مثيلاً بنصوص التشريع المصري الذي جاء خلوا من ذكرها.

– وفي المادة الرابعة تناول المشرع الكويتي فعل آخر يعد من الانتهاكات الخطيرة والمجرمة وهو حالة استخدام شبكة المعلومات أو أية وسيلة تقنية في التهديد أو الابتزاز لحمل الشخص على ارتكاب فعل أو الامتناع عنه، سواء أكان هذا التهديد بجناية أو مساس بكرامة الأشخاص أو خدشاً للشرف والاعتبار أو السمعة، وهو ذات ما أورده المشرع السعودي في الفقرة الثانية من المادة الثالثة حتى وإن كان هذا الفعل مشروعاً.

وجميعها حالات لم يرد لها مثيل في نصوص التشريعات المقارنة ونري أن المشرع الكويتي كان أكثر توفيقاً وحظاً من غيره في صياغة هذه النصوص، وندعو كل من المشرع المصري والسعودي والإماراتي إلى إتباع ذات النهج والتوسع في إدراج مثل هذه الحالات المتعلقة بتشديد العقوبة والمقترنة بجريمة الدخول غير المشروع.

---

(١) راجع الفقرة الثانية من المادة الرابعة من نظام مكافحة جرائم تقنية المعلومات السعودي .

(٢) تنص المادة (١١) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أن "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات.

ثالثاً: جريمة تجاوز حدود الحق في الدخول:

يقصد بها قيام أحد الأشخاص بالدخول إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول، وقد جاء النص علي هذه الجريمة في المادة ١٥ من قانون مكافحة جرائم التقنية المصري[١]، هذا وقد أفرد لها المشرع عقوبة مستقلة أخف وطأة عن سابقتها.

وبذلك فقد جعل المشرع المصري من حق الدخول المشروع المقرون بأفعال التجاوز عن حدود هذا الحق بالبقاء بعد المواعيد أو تجاوز مستوي الدخول جريمة مستقلة يعاقب فاعلها بعقوبة أخف وطأة عن سابقتها التي ترتكب حال الدخول غير المشروع، وهو مسلك لم يرد في تشريعات الدول المقارنة التي تناولتها ضمن جريمة الدخول غير المشروع ولم تتطرق أيا منها استقلالاً إلى حالة البقاء عقب انتهاء حالة الدخول المشروع، ونري من وجهة نظرنا أن هذه الجريمة هي تزايد غير مبرر، وكان يجب أن تدرج ضمن الجريمة سالفة البيان، وتأخذ ذات عقوبتها حتى وإن كانت ترتبط بحق مشروع مخول للجاني وهو حق الدخول المشروع .

(١) تنص المادة ١٥ على أن " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول ".

الفرع الثاني

جرائم الاعتداء على البيانات والنظم المعلوماتية

سعي المشرع من خلال تجريم أفعال الاعتداء أو التعدي على البيانات والمعلومات وكافة النظم المعلوماتية، سواء أخذ هذا التعدي شكل أتلاف أو تعطيل أو تعديل مسار أو إلغاء وسواء أكان هذا الإلغاء كلياً أم جزئياً، إلى توفير نوع من الحماية اللازمة لجميع وسائل وانظمه التقنية المعلوماتية من شبكات سلكية ولاسلكية وأجهزة ومعدات وبيانات وبرامج، وكذا أيضاً للمعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، وقد صنف المشرع هذا النوع من الجرائم إلى :

أولاً: جريمة الاعتراض غير المشروع:

يقصد بهذه الجريمة كل فعل ينطوي على اعترض يتم بدون وجه حق لأي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها. وقد جاء النص على هذه الجريمة في المادة السادسة عشر من القانون المصري[١]، كما تناولتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[٢].

هذا وقد حرص كل من المشرع الكويتي[٣]، والسعودي[١]، والإماراتي[٢]،

---

(١) تنص المادة ١٦ من قانون مكافحة جرائم تقنية المعلومات المصري على أن" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ".

(٢) يراجع المادة السابعة من الاتفاقية العربية الصادرة في شأن مكافحة جرائم تقنية المعلومات.

(٣) تنص الفقرة الثالثة من المادة الرابعة على أن " يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من تنصت أو التقط أو اعترض عمدا، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات ".

على إتباع ذات النهج بتجريم كل فعل ينطوي على اعتراض غير المشروع ومتعمد للبيانات والمعلومات المتداولة بوسائل التقنية المعلوماتية، أو الاعتراض غير المشروع والمتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

هذا وقد ضاعف كل من التشريع الكويتي[٣] والإماراتي[٤]، من حد العقوبة في حالة إذا ما أفشى الشخص ما تحصل عليه من معلومات عن طريق هذا الاعتراض .

ثانياً: جريمة الاعتداء على تصميم موقع:

تعد هذه الجريمة من أحدث الجرائم التي رصدتها بعض التشريعات الحديثة، وقننت لها نصوصاً عقابية وتجريميه مستقلة، وكان من بين هذه التشريعات بل وأهمها التشريع المصري الذي تناول هذه الجريمة في المادة التاسعة عشر منه، وأسهب في ذكر الأفعال التي تعتبر انتهاك أو اعتداء على تصاميم موقع خاص

---

(١) تنص الفقرة الأولي من المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات السعودي على أن "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه....." .

(٢) تنص الفقرة الأولي من المادة الخامسة عشر من القانون الإماراتي على أن يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمدا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية .

(٣) تنص الفقرة الثالثة من المادة (٤) من القانون الكويتي على أنه " .... فإذا أفشى ما توصل إليه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين".

(٤) تنص الفقرة الثانية من المادة ١٥ من القانون الإماراتي على أنه " ... فإذا أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة ".

بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق [١].

وقد سار كل من التشريعين الكويتي[٢]، والسعودي [٣] على ذات نهج المصري بتجريم هذه الأفعال والسلوكيات المتعلقة بالاعتداء على تصاميم موقع سواء أكان مملوكاً ملكية خاصة لشخص طبيعي أو شركة أو مؤسسة أو منشأة.

أما بالنسبة للتشريع الإماراتي فلم يختلف الأمر كثيراً عن تشريعات سابقيه، حيث تناولت المادة الخامسة منه التأكيد على معاقبة كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه[٤]، إلا أنه يؤخذ عليه تناوله تجريم هذه الأفعال والسلوكيات دون تحديد مدة عقوبة الحبس المقررة على مرتكبي هذه الجريمة على غرار ما فعلته التشريعات المقارنة التي تناولت تحديد مدة الحبس والغرامة بحديهما الأدنى والأقصى على النحو سالف البيان .

وفي جميع الأحوال يؤخذ على كافة هذه التشريعات قيامها على النحو المتقدم

---

(١) تنص المادة ١٩ من التقنين المصري على أن" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو أخفى أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق".

(٢) تنص الفقرة الثانية من البند (٢) من المادة الرابعة من التقنين الكويتي على أن " يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ".. ٢- أدخل عمدا عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها، أو دخل موقعا في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه أو إيقافه أو تعطيله.

(٣) تنص الفقرة ٣ من المادة الثالثة من التشريع السعودي على أن " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أياً من الجرائم المعلوماتية الآتية:.....٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه ".

(٤) تنص المادة الخامسة من التشريع الإماراتي على أن " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه".

بتناول هذه الجريمة بشكل مستقل في نصوص خاصة تتعلق بها في حين أن طبيعة هذه الجريمة تتشابه إلى حد كبير مع جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، ولا تخرج عن نطاقها، فكان من المتعين إدراجها ضمن هذه جريمة دون الحاجة لأن تدرج في نصوص خاصة بها.

ثالثاً: جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

لم يضع المشرع تعريفاً محدداً لهذه الجريمة، وإنما اكتفي بأن أشار في المادة ٢٠ من قانون تقنية المعلومات المصري[١] إلى بيان صور وأساليب ارتكابها، والتي يمكن من خلالها وضع تعريف لهذه الجريمة بأنها كل فعل يصدر من أحد الأشخاص ويمثل انتهاك لخصوصية موقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفه الدولة أو لحسابها أو لحساب أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها، سواء أخذ شكل الاعتداء، أو الاختراق، أو الدخول إليها، وسواء كان هذا الدخول متعمداً، أو بخطأ غير عمدي وبقى به بدون وجه حق، أو تجاوز حدود هذا الحق من حيث الزمان أو مستوى الدخول.

وقد تشدد المشرع المصري في الفقرة الثانية من ذات المادة وضاعف من حد العقوبة في حالة إذا ما كان هذا الدخول قد تم بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية[٢]، وجاءت الفقرة الثالثة من ذات المادة أكثر تشدداً في حالة إذا ما ترتب علي هذه الأفعال إتلاف للبيانات أو

---

(١) تنص الفقرة الأولي من المادة ٢٠ من القانون المصري على أن " يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو بخطأ غير عمدي وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتياً يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها ".

(٢) تنص الفقرة الثانية من المادة ٢٠ من ذات القانون على أن "... فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه".

المعلومات أو الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليا أو جزئيا، بأي وسيلة كانت[1].

ولم نجد لمثل هذا النمط أو الشكل الإجرامي صدي بالنصوص والتشريعات المقارنة، حيث لم تتناول النص صراحة على تجريم مثل هذا النوع من الاعتداء التي تقع على البيانات والأنظمة المملوكة للدولة، بل تناولت فقط تجريم فعل الدخول غير المشروع وما يترتب عليه من تعديات بشكل عام دون التطرق إلى كون هذه الاعتداءات أو الانتهاكات تنصب على نظام معلوماتي خاص بالأشخاص أم بنظام حكومي خاص بالدولة، وقد اكتفي البعض منها بالإشارة إلى مجرد تشديد العقوبة إذا ما كان الاعتداء قد وقع على نظام حكومي أو بيانات ومعلومات حكومية.

ومن بين هذه التشريعات التشريع الإماراتي الذي أشار إلى مجرد تشديد العقوبة حال ما وقع الاعتداء على نظام أو بيانات أو معلومات حكومية، ولم يأتي هذا التشريع بأي جديد بخصوص هذه الجريمة، ولم يتناول النص عليها بشكل مباشر وصريح مثلما فعل المشرع المصري، إنما يفهم اتجاه المشرع الإماراتي نحو تجريم هذه الأفعال من خلال ما ورد في المواد من (٢ : ٤) من قانون التقنية المعلوماتية الإماراتي والتي تتعلق بجرائم الدخول غير المشروع – سالفة الذكر– التي تناولت التجريم بشكل عام دون تحديد ما إذا كانت أفعال الاعتداء أو الانتهاك

(١) تنص الفقرة الثالثة من المادة ٢٠ من ذات القانون على أن "...، وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليا أو جزئيا، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه ".

المجرم وقعت على أنظمة مملوكة ملكية شخصية أم مملوكة للدولة أو الحكومة[١]، واكتفي في البند رقم (٣) من المادة الثانية منه بتشديد حد العقوبة المقررة لهذه الأفعال في حالة ما إذا انصب الاعتداد على بيانات أو معلومات شخصية[٢]، عكس ما هو متبع لدي المشرع المصري في شأن هذه الجريمة، كما أشار في المادة الثالثة من ذات القانون إلى ضرورة تشديد العقوبة أيضاً في حالة أخري، وهى حالة ما إذا وقعت الجريمة من موظف أثناء تأدية وظيفته أو بسببها[٣].

وتعتبر المادة الرابعة من التشريع الإماراتي من أكثر النصوص دلالة وتوافقاً مع ما نص عليه المشرع المصري من تجريم هذه الأفعال، المتمثلة في فعل الدخول بدون تصريح إلى أي موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[٤].

وقد وضاعف المشرع من حد العقوبة في حالة إذا ما تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو

---

(١) ينص البند ١ من المادة الثانية من القانون الإماراتي على أن " ١- يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة ".

(٢) ينص البند ٣ من المادة الثانية من القانون الإماراتي على أن:" ٣- تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة ٢ من هذه المادة شخصية ".

(٣) يراجع نص المادة الثالثة من القانون الإماراتي سالف البيان.

(٤) يراجع نص المادة الرابعة من القانون الإماراتي سالفة البيان.

النسخ أو النشر أو إعادة النشر[١].

وقد سايره في هذا الاتجاه المشرع الكويتي حيث لم يتناول أيضاً النص صراحة على هذه الجريمة أو الإشارة لفعل التجريم بشكل مباشر، وإنما أورد بعض الإشارات في نصوص متفرقة يفهم منها حظر هذه الأفعال دون النص على ما إذا كانت البيانات حكومية أو غير حكومية، وفي المادة الثالثة أشار إلى تشديد العقوبة في حال ما إذا كانت البيانات محل الاعتداء حكومية أو متعلقة بحسابات العملاء في المنشآت المصرفية[٢].

رابعاً: جريمة الاعتداء على سلامة الشبكة المعلوماتية:

تقضي المادة (١/ ٢١) من قانون مكافحة جرائم تقنية المعلومات المصري بمعاقبة كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين[٣].

---

(١) العقوبة المقررة في هذه الحالة السجن مدة لا تقل عن خمس ٥ سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ٢ مليون درهم، يراجع نص المادة الرابعة من القانون الإماراتي سالفة البيان.

(٢) ينص البند رقم (١) من المادة الثالثة من القانون الكويتي على أن " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ..... ١- ارتكب دخولا غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون. فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين . ويسرى هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية .

(٣) يراجع نص الفقرة الأولي من المادة ٢١ من قانون مكافحة جرائم تقنية المعلومات المصري.

وإذ البين مما سبق أن المشرع توسع في فرض الحماية التشريعية على وسائل تقنية المعلومات لاسيما الأنظمة والشبكات المعلوماتية، وكان حريصاً على حمايتها من كل ما يمكن أن يعيقها معدداً الأفعال التي قد تتسبب في الأضرار بها أو تهدد سلامتها و تعيق عملها أو تبطئ من سرعتها، أو تحد من كفاءتها، أو تشوش عليها بأي وسيلة من شأنها إحداث ذلك مما قد يتسبب في مخاطر وأضرار يصعب تداركها أو علاجها مستقبلاً، بل أنه قد يستحيل ذلك، ووضع لهذه الأفعال الإجرامية عقوبة رادعة في الفقرة الأولي من المادة ٢١ على النحو سالف البيان.

وبهذا النص يكون المشرع المصري قد فطن لنوع غاية في الأهمية والخطورة من الجرائم التقنية وتنبه لها قبل حدوثها وهي جرائم الاعتداء على سلامة الشبكة المعلوماتية، حتى وإن كانت هذه الجريمة تتشابه إلى حد كبير مع ما سبق عرضه من جرائم الاعتداء التقني، إلا أنه يعد اتجاه محمود وموفق، خاصة وأن هذا النص سالف البيان يتفق مع ما جاء في المادتين ٣١، ٥٧ من الدستور المصري لعام ٢٠١٤[١]، بل يعتبر هذا النص امتداداً وإعمالاً وجيهاً لما جاء بهذه النصوص الدستورية.

والجدير بالذكر أن المشرع أشترط لتطبيق العقوبات الواردة في الفقرة الأولي من المادة ٢١ من القانون سالفة البيان ضرورة أن تكون هذه الأفعال قد ارتكبت عن عمد وبقصد الإضرار، أما وإن وقعت هذه الجريمة دون عمد، وبخطأ من الجاني، فقد أعتبرها المشرع المصري من قبيل الأعذار المخففة للعقوبة، وأورد لها نص خاص في الفقرة الثانية من ذات المادة وجعل لها عقوبة أخف حدة عن

(١) تنص المادة ٣١ من الدستور المصري على أن" أمن الفضاء المعلوماتى جزء من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليها، على النحو الذي ينظمه القانون". كما نصت الفقرة الثالثة من المادة ٥٧ على أن"..، كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

سابقتها[١].

أما إذا وقعت هذه الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها، هنا فقد ضاعف المشرع من حد العقوبة المقررة لها لتصبح السجن المشدد، والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه[٢].

ولم يذهب المشرع السعودي بعيداً عن ذلك، فقد تناول في الفقرتين الثانية والثالثة من المادة الخامسة النص على ذات الأفعال الوارد ذكرها بالتقنين المصري وزاد عليها واعتبرها من قبيل الأفعال الإجرامية الخطرة واجبة العقاب[٣].

وقد سايرهم في ذلك المشرع الكويتي في المادة الرابعة منه[٤]، ولكنه كان غير موفق في الصياغة القانونية، حيث يؤخذ عليه في هذه المادة إغفال وعدم ذكر بعض الأفعال والسلوكيات التي تؤدي إلى وقوع الجريمة مثل فعل التشويش أو محاولة الحد من كفاءة عملها أو إعاقتها أو اعتراض عملها أو قيام الجاني بإجراء معالجة إلكترونية للبيانات الخاصة بالشبكة المعلوماتية بدون وجه حق أسوة بما فعله المشرع المصري على النحو المتقدم. وبالنسبة لموقف المشرع الإماراتي أيضاً فلم يختلف كثيراً عما ذهب إليه المشرع الكويتي من عدم التوسع

---

(١) تنص الفقرة الثانية من المادة ٢١ على أن" يعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين".

(٢) راجع نص الفقرة الثالثة من المادة ٢١ من ذات القانون المصري المشار إليه.

(٣) تنص المادة الخامسة من النظام السعودي على أن" يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- .....٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها. ٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

(٤) يراجع نص المادة الرابعة من القانون الكويتي الصادر في شان مكافحة جرائم تقنية المعلومات سالفة البيان.

في ذكر الأفعال والانتهاكات التي تمثل اعتداء على سلامة الشبكة المعلوماتية، وأغفل أيضاً ذكر البعض منها[١].

خامساً: الجرائم المرتكبة من مدير الموقع:

لما كنت طبيعة الوسائل التقنية وخصائصها الفنية المعقدة تحتاج إلى مزيد من الدقة والذكاء التقني والخبرة الفنية المعلوماتية الخاصة للتعامل معها، فبالتالي يصعب على الشخص العادي أو الهاوي أن يرتكب جرائم معلوماتية من النوع التقني – إلا في أضيق الحدود – فالأمر يحتاج إلى شخص ذو طبيعة خاصة يتمتع بذكاء تقني وخبرة فنية لارتكاب مثل هذا النوع من الجرائم المعلوماتية وكشف العقبات الفنية والتقنية التي أوجدها المتخصصون في مجال تقنية المعلومات لحماية أنظمتها من الاختراق.

ولما كان مدير الموقع هو كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع[٢] أو أكثر على الشبكة المعلوماتية، بما في ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه[٣] لذا فإن مدير الموقع هو أكثر الأشخاص قدرة على ارتكاب الجريمة لعلمه بكافة التفاصيل والثغرات الفنية المتعلقة بالموقع أو المجال المعلوماتى .

وإنطاقاً من هذا الدور الهام الذي يلعبه مدير الموقع أو المسئول عن إدارته

---

(١) تنص المادة العاشرة من القانون الإماراتي على أن يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من ادخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات ، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات .

(٢) الموقع: هو كل مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة. يراجع في هذه التعريفات نص المادة الأولي من قانون مكافحة تقنية المعلومات المصري.

(٣) يراجع في تعريف مدير الموقع المادة الأولي من قانون مكافحة تقنية المعلومات المصري.

فقد تنبه له المشرع المصري وسلك طريقاً واتبع نهجاً لم نري له مثيلاً بتشريعات الدول المقارنة حينما نص في المواد (٢٧ – ٣٥) من الفصل الرابع من القانون على معاقبة كل مسئول عن الإدارة أو الإشراف على موقع أو بريد اليكتروني أو نظام معلوماتي، طالما تسبب بخطئه أو أهمل أو تقاعس عن هذه المسئولية ونتج عنها تعريض هذه الوسيلة للانتهاك أو الإضرار، وتناول المشرع تقسيم العقوبات المقررة للجرائم التي تقع من المسئول أو مدير الموقع بحسب طبيعة الأفعال الإجرامية التي يقوم بها وخطورتها .

وفي هذا الصدد نشيد بالمسلك المتبع من المشرع المصري، وبالصياغة القانونية التي تبناها، وبالنسبة للتشريعات المقارنة الصادرة في ذات الشأن تبين خلوها جميعاً من تجريم مثل هذه الأفعال التي تصدر من المسئول أو المدير الذي تولي الإدارة الفعلية لهذه الوسائل التقنية، وندعو مشرعي الدول المقارنة جميعاً لأن يسلكوا ذات مسلك المشرع المصري وتخصيص نصوص عقابية لتجريم الفعل الواقع من المسئول عن إدارة المواقع والأنظمة المعلوماتية.

الفرع الثالث

جرائم الاحتيال المالي والحيازة والاتجار غير المشروع

بوسائل تقنية المعلومات

تنقسم هذه الطائفة من الجرائم إلى نوعين، جرائم الحيازة والاتجار غير المشروع بوسائل تقنية المعلومات، وجرائم الاحتيال المالي، وهى كما يلي:

أولاً: جرائم الحيازة والاتجار غير المشروع بوسائل تقنية المعلومات:

تناول المشرع المصري في المادة ٢٢ منه تجريم أفعال الحيازة والاتجار للوسائل التقنية المشار إليها ونص على معاقبة كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء"[١].

ويؤخذ على المشرع المصري تناوله هذه الأفعال الإجرامية تحت عنوان البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات، أى عدم توفيقه في صياغة المسمي التجريمي لهذه الأفعال الإجرامية أو الجريمة التقنية، فلم يتمكن من حسن اختيار المسمي المناسب الذي يمكن أن يدرج تحته هذه الأفعال والسلوكيات الإجرامية، واكتفي بتحديد الأفعال والسلوكيات المجرمة فقط دون اختيار العنوان المناسب والشامل لهذه الأفعال الإجرامية وبالتالي أنكر

(١) وقد عاقب المشرع مرتكبي هذه الافعال بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

تجريمها، وأري أنه كان من المتعين عليه أن يطلق عليها جرائم الحيازة والاتجار غير المشروع بوسائل تقنية المعلومات أو جريمة تسهيل الحصول على الوسائل والمعدات المستخدمة في ارتكاب الجريمة، أو جريمة إساءة استخدام وسائل تقنية المعلومات.

وسار على نهجه المشرع الإماراتي بتناوله هذه الجريمة في الفقرة الثانية من المادة الرابعة عشر من قانون مكافحة جرائم تقنية المعلومات[١]، إلا أنه يؤخذ عليه إغفاله للعديد من الأفعال التي وردت في التشريع المصري وتعد من قبيل الجرائم منها أفعال الحيازة والإحراز أو الجلب أو التصنيع على الرغم من أهميتها جميعاً، إضافة إلى أنه لم يتناول النص علي تجريم استخدام تلك الوسائل في إخفاء أثار الجريمة وأدلتها.

أما على الجانب السعودي: فقد أغفل المشرع الإشارة إلي هذه الجريمة ولم يتناول النص عليها صراحةً، حتى وإن قيل أنه أورد في المادة السادسة منه فعلي الإنتاج والإنشاء للبيانات والمواقع، فهذه الإشارة من وجهة نظرنا غير كافية ولا توحي بصراحة اتجاه المشرع السعودي نحو تجريم هذه السلوكيات والأفعال، وبالتالي يعاب عليه اتخاذه لهذا المسلك فهذه الأفعال تنطوي علي خطورة بالغة إن حدثت سوف ترتب أثار يصعب تداركها.

وفي التشريعي الكويتي: تلاحظ أنه تناول هذه الأفعال الإجرامية في الفقرة (٤) من المادة الرابعة من قانون مكافحة جرائم التقنية[٢]، ولكنه اشترط أن تؤدي

---

(١) تنص الفقرة الثانية من المادة الرابعة عشر على أنه: "....، ويعاقب بذات العقوبة كل من اعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع إلكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون.

(٢) تنص الفقرة (٤) من المادة الرابعة من القانون الكويتي الصادر في شان مكافحة جرائم تقنية المعلومات على أن "يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من:..... ٤- كل من أنشأ موقعا أو نشر أو أنتج

هذه الأفعال إلى المساس بالآداب العامة أو إدارة مكان لهذا الغرض، أي أنه خصص هذه السلوكيات وربطها بضرورة أن تستخدم بقصد المساس بالآداب العامة، فهي بذلك اعتبرها من قبيل الآثار الأخلاقية المتعلقة بجرائم الآداب، وهو اتجاه مغاير لما ذهب إليه المشرع المصري الذي تناول النص على هذه الأفعال والسلوكيات بشكل عام طالما ترتب عليها ارتكاب أية جريمة من الجرائم الواردة في القانون دون تحديد نوع وطبيعة الجريمة المرتكبة، وهو اتجاه محمود من المشرع المصري.

لذا أدعو المشرع الكويتي أن يتبني ذات الاتجاه ويقوم بحذف عبارة أن تستخدم في المساس بالآداب العامة ويستبدلها بعبارة " وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون".

كما ندعوه أيضاً أن يتوسع في ذكر الأفعال الإجرامية المتعلقة بهذا الجانب، ويحذو حذو المشرع المصري في هذا الشأن مثل إضافة فعل (حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول)، أو إقرار نص خاص بهذه الجريمة بشكل مستقل أسوة بالمشرع المصري.

ثانياً: جرائم الاحتيال المالي:

ورد النص على هذه الجريمة في الفقرة الأولي من المادة ٢٣ من قانون مكافحة جرائم تقنية المعلومات المصري تحت عنوان جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني، وهي عبارة عن مجموعة من الأفعال التي تمثل اعتداء وانتهاك لحقوق وخدمات مالية، من خلال

أو أعد أو هيأ أو أرسل أو خزن معلومات أو بيانات بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وكان ذلك من شأنه المساس بالآداب العامة أو أدار مكانا لهذا الغرض.

استغلال أو استخدام إحدى وسائل تقنية المعلومات، وكان ذلك بهدف الوصول دون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكتروني، حتى وإن لم يتحقق من وراءها ربح أو منفعة للجاني[١].

وقد تشدد المشرع وضاعف من حد العقوبة في حالة إذا ما كان الهدف والمقصد من وراء تلك الأفعال والانتهاكات هو السعي للحصول على أموال الغير أو ما تتيحه من خدمات[٢]، أما إذا توصل الجاني فعلياً من وراء هذه الأفعال إلى تحقيق مقاصده والاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير، هنا فقد ضاعف المشرع أيضاً من الحد الأقصى للعقوبة المقضي بها[٣].

وهو ذات ما تبناه المشرع الكويتي في المادة الخامسة من قانون التقنية الكويتي[٤]، وفي الفقرة (٥) من المادة الثالثة منه عاقب كل من توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء

---

(١) تنص الفقرة الأولي من المادة ٢٣ من التشريع المصري الصادر في هذا الشأن على أن " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية.

(٢) تنص الفقرة الثانية من المادة ٢٣ سالفة البيان على أن "....، فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

(٣) تنص الفقرة الثالثة من ذات المادة سالف البيان على أن "....، وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

(٤) تنص المادة الخامسة من قانون التقنية الكويتي على أن" يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن ألف دينار ولا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية. فإذا ترتب على استخدامها الحصول على أموال الغير، أو على ما تتيحه هذه البطاقة من خدمات، يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند، إلا أنه أشترط لتحقق ذلك ضرورة أن يتم من خلال استعمال طريقة احتيالية أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه[١].

وسايره في ذلك المشرع السعودي في المادة الرابعة بفقرتيها الأولي والثانية[٢]، أما المشرع الإماراتي فقد كان أكثر توسعاً وتوافقاً إلى حد كبير مع ما ذهب إليه المشرع المصري، وأولي لهذه الجريمة اهتماماً خاصاً، حينما تناولها في المادتين ١٢[٣]، ١٣[١] من قانون مكافحة جرائم التقنية المعلوماتية، بل يعتبر

---

(١) تنص الفقرة (٥) من المادة الثالثة من النقنين الكويتي على أن" يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من:..، ٥- توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند، وذلك باستعمال طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

(٢) تنص المادة الرابعة من القانون السعودي على أن "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :

١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .

٢- الوصول- دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات .

(٣) تنص المادة ١٢ من القانون الإماراتي على أن "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني.

وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير، أو الاستفادة مما تتيحه من خدمات.

فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين .

المشرع الإماراتي أكثر تميزاً عن سابقيه من أصحاب التشريعات المقارنة، بل عن المشرع المصري ذاته، وكان موفقاً في الصياغة القانونية لهذه النصوص، كما أنه تناول النص على جريمة لم يفطن لها المشرع المصري وهي جريمة النشر وكشف سرية البيانات والأرقام الائتمانية الواردة بالفقرة الأخيرة من المادة ١٢ سالفة البيان[٢].

ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني .

(١) تنص المادة ١٣ من ذات القانون على أن " يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة، أو أي وسيلة أخرى من وسائل الدفع الإلكتروني، وذلك باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي، ويعاقب بذات العقوبة كل من :

١- صنع أو صمم أي وسيلة من وسائل تقنية المعلومات، أو برنامج معلوماتي، بقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة .

٢- استخدم بدون تصريح بطاقة ائتمانية أو إلكترونية أو بطاقة مدينة أو أي وسائل أخرى للدفع الإلكتروني، بقصد الحصول لنفسه أو لغيره، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير .

٣- قبل التعامل بهذه البطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني مع علمه بعدم مشروعيتها .

(٢) يراجع نص الفقرة الأخيرة من المادة ١٢ من التشريع الإماراتي سالفة البيان .

المطلب الثاني

الجرائم المتعلقة بالبريد الالكتروني

والمواقع أو الحسابات الخاصة

تمهيد:

لقد كان المشرع المصري حريصاً على حماية حقوق وحريات الإنسان وخصوصياته من آية انتهاكات قد تتعرض لها وكان ذلك واضحاً وجلياً بإصداره قانون مكافحة جرائم تقنية المعلومات، وحدد لكل فعل إجرامي يمثل انتهاك أو إهدار لحريات وخصوصية الإنسان عقوبة تتناسب وخطورة الفعل الإجرامي المرتكب، وتنقسم هذه النوعية من الجرائم إلي طائفتين، الطائفة الاولي طائفة جرائم الاعتداء على البريد الالكتروني والمواقع أو الحسابات الخاصة، الطائفة الثانية طائفة الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، وهو ما سنتناوله تفصيلاً فيما يلي:

تقسيم:

سوف نقوم بتقسيم الدراسة في هذا المطلب الى فرعين كما يلي:

الفرع الأول: جرائم الاعتداء على البريد الالكتروني والمواقع أو الحسابات الخاصة.

الفرع الثاني: الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني.

الفرع الأول

جرائم الاعتداء على البريد الإلكتروني

والمواقع أو الحسابات الخاصة

تلاحظ في الآونة الأخيرة كثرة الانتهاكات والاعتداءات الموجهة لوسائل التواصل الاجتماعي بما فيها البريد الالكتروني E-Maile[1]، والمواقع والحسابات الخاصة الشخصية، وتعرضها لمحاولات التعدي عن طريق سرقتها أو اختراقها، وكشف سريتها، وسرقة محتواها، وقد يصل الأمر نتيجة هذه الانتهاكات إلى ابتزاز مالكيها وتهديهم، مما دعي إلى ضرورة التدخل التشريعي لحماية هذه الوسائل التقنية ومواقع للتواصل الاجتماعي من مثل هذه الاعتداءات وفرض عقوبات رادعة .

وكان المشرع المصري من أكثر مشرعي دول العالم حرصاً على حماية هذه الوسائل التقنية من الانتهاكات والتعدي عليها بفرض عقوبات صارمة على مرتكبيها، حيث تناول في الفقرة الأولي من المادة الثامنة عشر تجريم كل فعل ينطوي على انتهاك لخصوصية البريد الالكتروني[2] أو المواقع أو الحسابات

---

(١) هو عبارة عن وسيلة اتصالية يتم بها إرسال واستقبال الرسائل الالكترونية أياً كان شكلها ومحتواها، وتعتبر الرسائل والمراسلات المرسلة عن طريق البريد الالكتروني من المراسلات الخاصة التي تستلزم استصدار إذن قضائي لضبطها لكونها من قبيل خصوصيات المتهم ومستقر أسراره، وفي ذلك تقول محكمة النقض المصرية " أن مدلول كلمتي الخطابات والرسائل التي أشير إليها وإباحة ضبطها في أي مكان خارج منازل المتهمين طبقاً للإحالة على الفقرة الثانية من المادة ٩١ إجراءات جنائية يتسع في ذاته لشمول كافة الخطابات والرسائل والطرود والرسائل التلغرافية، كما تندرج تحته المكالمات التليفونية لكونها لا تعدو أن تكون من قبيل الرسائل الشفوية". الطعن رقم١٨١٣ لسنة ٣٦ ق– جلسة ١٩٦٧/٢/١٤– مكتب فني ١٨، ج١. د/ تهاني السبيت– ما هو البريد الالكتروني، مقدمة دراسة منشورة على موقع الموسوعة العربية للكمبيوتر والانترنت، بتاريخ ٢٠٠١/١/٢١، ص١.

(٢) أحالة النيابة العامة أحد المتهمين للمحاكمة في القضية رقم ٦٦٩٢ لسنة ٢٠٠٤ إداري شبرا الخيمة أول – على خلفية قيامه في غضون عام ٢٠٠٤ بالاتي: " أولاً: قذف المجني عليها في علانية من خلال البريد الالكتروني عبر شبكة الانترنت بعبارات خادشة لشرفها واعتبارها وهي عبارات تضمنتها

الخاصة التي تؤول ملكيتها لأشخاص طبيعيين[١]، وضاعف المشرع في الفقرة الثانية من ذات المادة من حد العقوبة حال إن وقعت تلك الجريمة علي بريد إلكتروني أو مواقع أو حسابات خاصة تؤول ملكيتها لأشخاص اعتبارية خاصة[٢].

وعلى الجانب التشريعي المقارن، فقد تعدد الاتجاهات التشريعية وانقسمت إلى فئتين، منها ما أخذ بذات نهج المشرع المصري بتجريم هذه الأفعال، ومنها ما أغفل ذلك ولم يتناولها في تشريعاته وسلك بذلك مسلكاً مغايراً، وذلك على النحو التالي:

فقد سلك المشرع الإماراتي[٣] ذات مسلك المشرع المصري بالنص على

وحوتها احد عشر رسالة أرسلها إليها المتهم باستخدام شبكة الانترنت. ثانياً: تعمد مضايقة المجني عليها بإساءة استعمال جهاز من أجهزة الاتصالات البريد لالكتروني وأرسل إليها عبارات سب وقذف وصور فاضحة مخلة بالآداب العامة ومخدشة للحياء مما اضر بها ضرراً كبيراً . وفي القضية رقم ٦٨٥٤ لسنة ٢٠٠٣ م الحوامدية بجنايات الجيزة، ورقم ٣٢٦١ لسنة ٢٠٠٣ م كلي – المقضي فيها بجلسة ٢٠٠٤/١/١٨ بمعاقبة الجاني لقيامه بإنشاء موقعاً للمجني عليها على شبكة الانترنت وأرسل لها عبارات عبر التليفون المحمول وكذلك رسائل اليكترونية عبر البريد الالكتروني يراود به المجني عليها عن نفسها، وطلب منها دفع مبلغ خمسة آلاف دولار ولما استكثرت مثل هذا المبلغ اخبرها أنها تتخيل والدتها عندما تري صورها وكذلك زملائها في العمل .

(١) تنص الفقرة الأولي من المادة ١٨ من القانون المصري على أن " يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بآحاد الناس".

(٢) تنص الفقرة الثانية من المادة ١٨ من القانون المصري على أن ".....فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين".

(٣) قضت محكمة أبو ظبي الدائرة الأولي في القضية رقم ٤٣٧٣ لسنة ١٩٩٧ جنح أبو ظبي بجلستها المنعقدة في ١٩٩٧/١٢/٢ بإدانة المتهم ومعاقبته بغرامة قدرها عشرة آلاف درهم ومصادرة الصورة المضبوطة وإعدامها على خلفية قيام احد المشتركين بشبكة الانترنت (المتهم)– بأمارة أبو ظبي– ببث صورة لامرأة عارية وإرسالها إلى المشتركين الآخرين الذين تبدأ أسماؤهم بحروف XYZ، من خلال البريد الالكتروني الخاص بهم ونسب إليها كذباً أنها تبيع جسدها وتعرضه على راغبيه وكان ذلك بطريق العلانية وبالتالي تحقق أركان جريمة القذف. مشار إليه لدى د/ جميل عبد الباقي الصغير–

تجريم أفعال التعدي على البريد الالكتروني، والمواقع والحسابات الخاصة والشخصية وإن كان يؤخذ عليه عدم تحديده لأفعال التعدي المشار إليها وعدم وضوح النص وعيب الصياغة وعدم دقتها، كما أنه لم يفرق بين ما إذا كانت هذه الوسائل تؤول ملكيتها لأشخاص طبيعيين أم كانت تؤول لأشخاص اعتبارية.

حيث نص في المادة الثامنة على معاقبة كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني بعقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، وفي الفقرة الثالثة من المادة العاشرة منه تناول معاقبة كل من أرتكب عن عمد أي فعل يقصد به إعراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته بالحبس والغرامة أو إحدى هاتين العقوبتين، ويؤخذ عليه في هذه الفقرة عدم الوضوح ودقة الصياغة لعدم تحديد مدة عقوبة الحبس المقررة والواجب تطبيقها على هذه الجرائم .

وفي المادة الرابعة عشر من ذات القانون الإماراتي نص على تجريم الانتهاكات التي ترد على سرية المواقع والحسابات والأرقام السرية والشفرات وكلمات المرور أو أية وسيلة للدخول إلى هذه المواقع أو الشبكات والمعاملات بما فيها البريد الالكتروني، حيث نصت الفقرة الأولي من هذه المادة على أن "يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل، بدون تصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو معلومات إلكترونية" .

أما بالنسبة لكل من التشريعين الكويتي والسعودي فقد تبين لنا بالاطلاع عليها

الانترنت والقانون الجنائي– الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩، ص٤٣.

أن هذه التشريعات جاءت خلواً من مثل هذا التجريم ولم تتناوله لا من قريب أو من بعيد، فقد أصابها العجز والقصور في هذا الجانب، وندعوهما إلى ضرورة الإسراع في تدارك ذلك بتضمين تشريعاتهما نصوص عقابية تجريميه تتعلق بفعل التعدي وما يسببه من انتهاكات لوسائل التواصل الاجتماعي والمواقع والحسابات والبريد الالكتروني .

الفرع الثاني

الجرائم المتعلقة باصطناع المواقع

والحسابات الخاصة والبريد الإلكتروني

لقد أولي المشرع المصري وسائل التقنية الحديثة لاسيما وسائل التواصل الاجتماعي عناية خاصة، وعمل على إحاطتها بسياج واقي من التشريعات العقابية، وإضفاء نوع من الحماية التشريعية عليها ضد أية انتهاكات قد تصيبها، أو محاولة الاعتداء عليها أو استغلالها أو استخدامها في ارتكاب أياً من الجرائم التقنية، ومن بين أوجه الحماية التشريعية التي أوجدها المشرع المصري لهذه الوسائل ما تضمنته المادة ٢٤ من قانون مكافحة جرائم تقنية المعلومات، من حماية وسائل التقنية الحديثة ومواقع التواصل الاجتماعي من عمليات الاصطناع، حينما نصت على معاقبة كل من اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري(١).

وقد جاء هذا النص متوافقاً مع ما سبق وأن قضت به الدائرة الثانية الابتدائية بالمحكمة الاقتصادية ببني سويف، بحبس شخص ما لمدة ستة أشهر، وتغريمه مبلغ وقدرة عشرة آلاف جنيه لإساءته استخدام وسائل التواصل الاجتماعي وقيامه بالتعدي على أحد الأشخاص عن طريق السب والقذف الالكتروني باستخدام موقع "الفيس بوك"(٢)، ولا يغير من الأمر في شئ أن تكون إجراءات المحاكمة والعقاب

---

(١) تنص المادة ٢٤ سالفة البيان على أن:"يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين، كل من اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري. فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى ما نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين. وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، فتكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه.

(٢) وقد جاء في واقعات الدعوى رقم ٤٢٨ لسنة ٢٠١٧ جنح اقتصادي بني سويف، المقامة من النيابة العامة، ضد/.....، لاتهامه بالتعدي بالسب على مستشار عضو هيئة قضايا الدولة، وعلى أهله ووجه

قد تمت إعمالاً لحكم المادة ٧٦/٢ من القانون رقم ١٠ / ٢٠٠٣ الصادر بشأن تنظيم الاتصالات بدلاً من قانون مكافحة جرائم تقنية المعلومات نظراً للتشابه الكبير فيما بينها.

والجدير بالذكر أن المشرع في الفقرة الثانية من ذات المادة سالفة البيان ضاعف من حد العقوبة المقررة لهذه الجريمة في حالة ما إذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى ما نسب إليه[١].

إليهم ألفاظ خادشة والتي من شأنها خدش الشرف والاعتبار، وتعمد إزعاج ومضايقة غيره بإساءة استعمال أجهزة الاتصالات، من خلال السب والقذف من خلال مواقع التواصل الاجتماعي "فيس بوك"، وقيامه بإنشاء حسابين باسم "اتحاد محامى" و"ميار مصطفى" وبدأ في سب والقذف العلني للمجني عليه وشقيقه وإرسال شتائم لهما فى رسائل خاصة ونشر صور لأقاربهما مصحوبة بسباب وتشهير بهم على حسابه الشخصي.

وقالت المحكمة في حيثيات حكمها، إن الدعوى الجنائية انتهت إلى تعمد المتهم إزعاج المجني عليه بإساءة استعماله لوسائل الاتصالات، وثبوت تلك الجريمة في جانب المتهم، وأن الثابت للمحكمة أن التهمتين اللتين دانت المحكمة المتهم بهما تشكلان جريمتين متعددتين ارتكبتا لغرض واحد، وكانت هاتان الجريمتين مرتبطتان ببعضهما البعض ارتباطا لا يقبل التجزئة حيث إنهما مترتبتان على بعضهما البعض بحيث ما كانت ترتكب الجريمة التالية لولا وقوع التي تسبقها، وهو ما جاء في تعريف الارتباط في قانون العقوبات في الرأي الفقهي، وهو ما تطبق معه المحكمة عقوبة الجريمة الأشد لهاتين الجريمتين وهى عقوبة إساءة استخدام أجهزة الاتصالات، والمؤثمة بالمادة ٢/ ٧٦ من القانون رقم ١٠ لسنة ٢٠٠٣ بشأن قانون تنظيم الاتصالات والحكم بعقوبة تلك المادة التي تقضى معه المحكمة بمعاقبة المتهم.

(١) قضت المحكمة الاقتصادية بأن الثابت للمحكمة من مطالعتها لأوراق الجنحة عن بصر وبصيرة بعدما ألمت بها وبظروفها ومستنداتها ووازنت بين أدلة الاتهام ودفاع المتهم فرجحت أدلة الاتهام وثبت في يقينها قيام المتهم بارتكاب الجريمة الثابتة بالأوراق ثبوتاً لا يدع مجالاً للشك والريبة من قيامه بإنشاء صفحة على موقع التواصل الاجتماعي الفيس بوك وضع عليها صورة خاصة للمجني عليها مما تسبب لها من أضرار ومضايقة وذلك كما هو ثابت من التقرير الفني أن المتهم هو الذي قام بإرسال الرسائل على الموقع المنشأ بمعرفته وتطمئن المحكمة لأقوال المجني عليها وكذلك لتقرير الفحص الفني الأمر الذي تطمأن معه المحكمة بثبوت الاتهام في حق المتهم، ولما كانت الجرائم المسندة إلى المتهم قوامها فعل مادي واحد هو قيامه بإنشاء حساب على موقع الفيس بوك بشبكة المعلومات الدولية الإنترنت يحمل اسم/ .... وعليه عدد صورة شخصية خاصة بها بملابس المنزل الداخلية وتعمد إزعاج ومضايقة المجني عليها بإساءة استعمال وسائل الاتصالات وذلك بأن قام بنقل صورة شخصية لها

ومن الملاحظ على هذه الفقرة التي ضاعف فيها المشرع من حد العقوبة، أن المشرع من جهة نظري قد وقع في خطأ مادي في عبارة أمر يسئ إلى ما نسب إليه، بدلاً من عبارة أمر يسئ إلى من نسب إليه، وإن كان هذا الخطأ غير مقصود إلا أنه قد أصاب هذه الفقرة بالخلل، ويجب على المشرع السعي نحو تداركه واستبدال (من نسب إليه) بدلاً من (ما نسب إليه).

وفي الفقرة الثالثة من ذات المادة اتجه المشرع إلى التشدد في معاقبة الجاني حال إذا ما وقع الاعتداء على شخص اعتباري عام، ونعيب على المشرع في هذه الفقرة الأخيرة أنها – من وجهة نظرنا – تعتبر من قبيل التزيد غير المبرر، فكان من المتعين إدراجها ضمن الفقرة الأولي من ذات المادة حتى وإن قيل أن الفقرة الأولي تشير إلى نسبة الموقع المزور إلى شخص اعتباري، أما الفقرة الثالثة تشير إلى ارتكاب فعل التعدي على الشخص الاعتباري ذاته وليس نسبته إليه، فكلاهما يصب في ذات المعني .

أضف إلى هذه الانتقادات، أن المشرع المصري – من وجهة نظري – قد أصرف وتزايد في النص على هذه الجريمة، حيث كان من المتعين إدراجها ضمن الجريمة الواردة في نص المادة ١٨ من القانون والمتعلقة بالاعتداء على البريد الالكتروني أو المواقع أو الحسابات الخاصة، بحيث يضاف إلي فعل الاعتداء المجرم فعل الاصطناع، دون الحاجة للنص عليها استقلالاً والوقوع في هذا التزيد والاسترسال غير المبرر.

ولم نري في تشريعات الدول المقارنة صدي لمثل هذه الحماية التشريعية،

بملابس داخلية وقام بوضعها على شبكة المعلومات الدولية الإنترنت ولا ينال من ذلك إنكار المتهم لارتكابه الفعل الإجرامي مما تتحقق به حالة التعدد المعنوي الذي يوجب تطبيق نص المادة ٣٢ من قانون العقوبات ومعاقبة المتهم بالجريمة الأشد الأمر الذي نرى معه المحكمة بناء على نص المادة ٣٢ من قانون العقوبات أنه هناك ارتباط معنوي بين قيام المتهم بنقل صورة شخصية لها بملابس داخلية وقام بوضعها على شبكة المعلومات الدولية الإنترنت والإساءة إلى المجني عليها مما تقضي معه المحكمة بمعاقبته بنص الجريمة الأشد والمنصوص عليها بالمادة ٢/ ٧٦ من قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣. الحكم رقم ١٦٧ لسنة ٢٠١٣ – تاريخ الجلسة ١٨ /٧/ ٢٠١٣ م.

حيث لم يتناول أياً من هذه التشريعات المقارنة النص على مثل هذه الأفعال التي تمثل جريمة من جرائم الاعتداء التقني، كما لم يرد بنصوصها أية أشارة تفيد الاتجاه نحو تجريم فعل الاصطناع القني لمواقع أو حسابات خاصة أو بريد إلكتروني أسوة بما جاء بنصوص قانون التقنية المصري على النحو المتقدم.

المطلب الثالث

جرائم الاعتداء على حرمة الحياة الخاصة

وانتهاك الخصوصية

لا جدال في أن المشرع المصري كان ولا زال حريصاً على حماية الحقوق والحريات حرصاً عظيماً لاسيما حق الإنسان في الحياة الخاصة[١]، والعمل على مواجهة كل ما ينطوي عليه استخدام وسائل التقنية الحديثة من انتهاكات وتهديدات للحق في الخصوصية، فلم يكتفي المشرع المصري بإفراغ ذلك الاهتمام في نصوص قانونية، وإنما تخطي ذلك إلى أن ضمنه في نصوص دستورية ضمن نصوص الدستور المصري لعام ٢٠١٤، وعمل على إحاطتها بحماية خاصة ضد أية انتهاكات قد تحدث من وسائل التقنية المعلوماتية، ومنها الاهتمام بالحفاظ على سرية المحادثات والمراسلات البريدية وغيرها من وسائل الاتصالات والمعلومات، وحظر رقابتها أو وقفها أو تعطيلها أو الحد من كفاءتها أو التنصت عليها إلا بأمر قضائي[٢]، نظراً لما تسببه هذه التعديات من تهديد لمنظومة الاقتصاد والأمن القومي[٣].

---

(١) لم يتفق الفقه القانوني على وضع تعريف منضبط ومحدد للحياة الخاصة، أو ما يسمى بحق الإنسان في الخصوصية، بل أن كافة الاجتهادات الفقهية التي قيلت في هذا الشأن جاءت متعددة ومتباينة فيما بينها، ومقترنة بالانسحاب من الوسط أو العالم المحيط، وهى تتشابه إلى حد كبير بفكرة الخلوة أو العزلة، والبعض تناولها على أنها حق الشخص في أن يترك وشأنه، وإزاء هذه الصعوبة والتعددية التي واجهت الفقه القانوني في وضع تعريف محدد جامع مانع للحق في الحياة الخاصة، اتجه جانب عريض في الفقه القانوني إلى ترك هذا الأمر لسلطة القضاء في ضوء مجموعة من الأسس المستمدة من التقاليد والثقافات والقيم الدينية السائدة والنظام السياسي المعمول به في كل مجتمع بما يكفل للإنسان أن تُحترم ذاته مما يضمن له الهدوء والسكينة والأمن بمنأى عن الآخرين من التدخل في خصوصياته. د/ أسامة عبد الله فايد– الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩٢، ص١٥.

(٢) يراجع نص المادة ٥٧ من الدستور المصري لعام ٢٠١٤، سالفة البيان.

(٣) يراجع نص المادة ٣١ من الدستور المصري لعام ٢٠١٤، سالفة البيان.

وبإصدار قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ خصص المشرع المصري فصلاً خاصاً لمكافحة الجرائم التقنية التي تقع على حرية الإنسان وانتهاك خصوصيته تضمن في المادة ٢٥ منه تجريم كل فعل ينطوي على اعتداء يقع على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهاك حرمة الحياة الخاصة، أو القيام بإرسال رسائل الإلكترونية لشخص معين بكثافة دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقة صاحب الشأن، أو نشر معلومات أو أخبار أو صور وما في حكمها عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات يترتب عليها أن تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة[١].

وتطبيقاً لذلك اتجه كل من الفقه القانوني والقضاء في احدث أحكامه إلى تجريم كل فعل ينطوي على معاكسات أو أفعال غير مشروعة تؤدي إلى إزعاج أو مضايقات تتم بواسطة أو من خلال أي وسيلة من وسائل الاتصال سواء أكانت تليفون أو حاسب آلي أو بريد إليكتروني أو رسائل إلكترونية، وتركا للقاضي السلطة التقديرية الكاملة في تحديد الأفعال غير المشروعة وما إذا كانت هذه الأفعال المرتكبة تشكل إزعاجاً أو مضايقة للمتلقي من عدمه، فهي مسألة موضوعية تختلف من حالة إلى أخري[٢].

---

(١) تنص المادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات المصري على أن "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.

(٢) حكم المحكمة الاقتصادية الصادر في الجنحة رقم ٢٠٩٩ لسنة ٢٠١٨ – جلسة ٣٠/ ٨/ ٢٠١٨ – جنح طنطا لاقتصادية. وفي ذات السياق سبق وأن قضي بأنه بالدخول على عنوان البريد الإلكتروني

وإذ البين من مطالعة نص المادة ٢٥ سالفة البيان أنها تتوافق إلى حد كبير مع ما جاء في المادة (١٦٦) مكرر من قانون العقوبات المصري[١]، على الرغم من اختلاف نوع وحد العقوبة المقررة لفعل الإزعاج الوارد في كليهما، وفي المادة ٢٦ من ذات القانون ضاعف المشرع الحد المقرر للعقوبة إذا ما تعمد الجاني استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه[٢].

الخاص بالمواطن/..... وفحصه فنياً تبين الآتي: وجود رسالة مرسلة إلى عنوان البريد الإلكتروني الخاص به وهو .... من عنوان البريد الإلكتروني الخاص بالمواطنة/ ..... وهو ..... – بعنوان "من ....." صادرة من رقم تعريفي (البصمة الإلكترونية .... ip: 197.195.135.74 (بتاريخ 2012/4/20 الساعة 20:14:55 مساء بالتوقيت القاهرة .ولمعرفة مكان إرسال الرسالة يستعلم عن الأرقام التعريفية المشار إليها في التاريخ والوقت المحددين من شركة "....." وهو ما تطمئن معه المحكمة وثبت في يقينها قيام المتهم بارتكاب الجريمة الثابتة بالأوراق ثبوتاً لا يدع مجال للشك والريبة من قيامه وذلك كما هو ثابت من التقرير الفني أن المتهم هو الذي قام بإرسال الرسائل على موقع المجني عليها وقام بوضعها على شبكة المعلومات الدولية الانترنت ولا ينال من ذلك إنكار المتهم لارتكابه الفعل الإجرامي مما تتحقق به حالة التعدد المعنوي الذي يوجب تطبيق نص المادة ٣٢ من قانون العقوبات ومعاقبة المتهم بالجريمة الأشد الأمر الذي ترى معه المحكمة بناء على نص المادة ٣٢ من قانون العقوبات أنه هناك ارتباط معنوي بين قيام المتهم بتعمد إزعاج المجني عليها وسبها وخدش حياءها والإساءة إلى المجني عليها مما تقضي معه المحكمة بمعاقبته بنص الجريمة الأشد والمنصوص عليها بالمادة ٢/٧٦ من القانون رقم ١٠ لسنة ٢٠٠٣ بشأن الاتصالات وهو ما تقضي معه المحكمة بإدانته بالعقوبة الأشد المقررة في المادة سالفة الذكر عن التهم للارتباط وهو ما تقضي به المحكمة على نحو ما سيرد بالمنطوق. الحكم رقم ٥٧٥ لسنة ٢٠١٣– تاريخ الجلسة ٢٠١٣/٦/٢٦

(١) تنص المادة ١٦٦ مكرر قانون العقوبات المصري على أن "كل من تسبب عمداً في إزعاج غيره بإساءة استعمال أجهزت الاتصالات التليفونية يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تزيد على مائة جنية أو بإحدى هاتين العقوبتين".

(٢) تنص المادة ٢٦ من قانون التقنية المصري على أن " يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

وقد قضت محكمة القاهرة الاقتصادية- تطبيقاً لما سبق- بمعاقبة احدي شركات إبادة الحشرات بغرامة مالية لقيامها دون وجه حق وبالمخالفة للقانون بإرسال رسائل مزعجة للمواطنين وفقاً للمادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات الخاصة بحماية حرمة الحياة الخاصة، وذلك بناء على البلاغ المقدم للنيابة العامة من الجهاز القومي لتنظيم الاتصالات، ووجهت إلي هذه الشركة عدة اتهامات منها، إنشاء شبكة اتصالات واستخدامها في خدمة الرسائل الجماعية وإجراء الاتصالات وذلك دون ترخيص، استخدام وسائل غير مشروعة في إجراء خدمات الاتصالات، بالإضافة إلى تهم تعمد إزعاج المواطنين والانتفاع دون وجه حق، وحيازة برنامج مخالف للقانون واستخدامه، ومنح البيانات الشخصية للمواطنين لنظام إلكتروني للترويج عن السلع والخدمات دون الحصول على الموافقة منهم(١).

وهذا وقد سعت أغلب التشريعات المقارنة أيضاً لحماية هذه الخصوصية إلا أن البين أن اهتمامها كان اهتماماً محدوداً بالمقارنة بما آتاه المشرع المصري، فمنها المشرع السعودي الذي تناول في المادة الثالثة(٢)، والفقرة الأولي من المادة

---

(١) يراجع حكم محكمة القاهرة الاقتصادية الصادر في الجنحة رقم ٦٤٧ لسنة ٢٠١٩، والمؤيد بالحكم ألاستئنافي الصادر بجلسة ٢٠١٩/١٢/١٠. ويراجع في ذات المعنى أيضا حكم محكمة النقض- الدائرة الجنائية، في الطعن رقم ٧٨٤٣ لسنة ٨٧ ق- جلسة ٢٠١٩/١/٢٠.

(٢) تنص المادة الثالثة من التقنين السعودي على أن" يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .

٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها .

الخامسة[١] النص على حماية حرمة الحياة الخاصة وحق الإنسان في الخصوصية من أفعال التنصت على المراسلات البريدية الالكترونية أو اعتراضها، وكذا الدخول غير المشروع إلى مواقع إليكترونية بهدف التهديد أو الابتزاز أو إتلاف هذه المواقع والتصاميم أو استخدام الهواتف النقالة المزودة كاميرات في الإساءة والمساس بالحياة الخاصة والتشهير بالغير وإلحاق الضرر به، إضافة لما جاء بالمادة السادسة من حماية حق الإنسان من إنتاج ما من شأنه المساس بحرمة الحياة الخاصة[٢].

وبالنسبة للتشريع الكويتي فقد تناول النص على هذه الحماية التشريعية للحياة الخاصة في الفقرة الثالثة من المادة الثانية والتي تضمنت تشديد العقوبة إذا ما وقعت هذه الاعتداءات على بيانات أو معلومات شخصية[٣]، وفي الفقرة الرابعة

٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة .

(١) تنص الفقرة الأولي من المادة الخامسة من النظام السعودي على أن " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

(٢) تنص الفقرة الأولي من المادة السادسة من النظام السعودي على أن" يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي،.....".

(٣) تنص المادة الثانية من قانون مكافحة التقنية الكويتي على أن" يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من أرتكب دخولا غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية.

فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين. فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

من المادة الثالثة قام بمعاقبة كل من استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. وضاعف من حد العقوبة إذا كان التهديد بارتكاب جناية أو بما يعد مساسا بكرامة الأشخاص أو خادشا للشرف والاعتبار أو السمعة[١]. وفي المادة الرابعة تناول التأكيد على حظر وتجريم التصنت أو التجسس أو إعاقة للوصول إلى مواقع أو بيانات، أو اعتراض أية مراسلات تتم عن طريق الشبكة المعلوماتية أو وسيلة من وسائل التقنية المعلوماتية، أو قام بإفشائها أو نشرها للعامة، وكل ذلك يعد من قبيل الاعتداءات الواقعة على الحقوق الخاصة للأفراد[٢].

ويعتبر المشرع الإماراتي من أكثر التشريعات المقارنة اهتماماً بحماية حرمة الحياة الخاصة أسوة بالمشرع المصري، وقنن لها نصوصاً متعددة منها ما جاء بالفقرة الأولي من المادة ٢١ من القانون رقم ٥ لسنة ٢٠١٢ وتعديلاته التي تضمنت تجريم كل فعل يمثل اعتداء لخصوصية شخص ما يتم بواسطة استخدام احدي وسائل تقنية المعلومات أو الشبكات المعلوماتية، وقد عددت هذه الفقرة الطرق التي تمثل فعل اعتداء منها استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية، وكذا التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها . كما أدخل المشرع من ضمن هذه الأفعال نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية، وقد عاقب مرتكبي هذه الأفعال بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم

ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أيا من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته.

(١) راجع في ذلك نص الفقرة الرابعة من المادة الثالثة من قانون مكافحة تقنية المعلومات الكويتي.

(٢) راجع في ذلك نص المادة الرابعة من قانون مكافحة تقنية المعلومات الكويتي.

أو بإحدى هاتين العقوبتين[١].

وفي الفقرة الثانية من ذات المادة ٢١ ضاعف المشرع من حد العقوبة في حالة قيام الجاني باستخدام نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها"[٢] . أو قيامه بدون تصريح باستخدام أي شبكة معلوماتية، أو موقعا إلكترونيا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه [٣].

ويتبين مما سبق أن المشرع المصري يعد من أفضل مشرعي دول العالم حرصاً على حماية حرمة الحياة الخاصة، وتبعه في ذلك المشرع الإماراتي، ونشيد لهما بحسن الصياغة القانونية لهذه النصوص العقابية.

(١) راجع الفقرة الأولي من المادة ٢١ من القانون الإماراتي.
(٢) راجع الفقرة الثانية من المادة ٢١ من القانون الإماراتي.
(٣) راجع في ذلك نص المادة ٢٢ من قانون مكافحة تقنية المعلومات الإماراتي.

المبحث الثالث

الأحكام الإجرائية الخاصة بمكافحة الجرائم التقنية

تمهيد:

الأحكام الإجرائية هي عبارة عن مجموعة المبادئ والنصوص التي تحدد وتنظم الإجراءات الواجب إتباعها منذ لحظة ارتكاب الجريمة وحتى استيفاء حق الدولة في العقاب، ومع تصاعد حدة الإجرام المعلوماتى التقني وكثرة وقوعها كان من المتعين على المشرع العمل على مواجهة هذا الإجرام المتطور وفق قواعد إجرائية ملائمة تتواءم معه، الأمر الذي دعاه عند إصدار القانون رقم ١٧٥ لسنة ٢٠١٨ أن يكون حريصاً على سن وتنظيم مجموعة مناسبة من الأحكام الإجرائية اللازمة والواجب إتباعها لمكافحة الجريمة المعلوماتية، وعمل نوع من التوازن بين ممارسة الإنسان لحرياته وحقوقه التي تواكب التطور التكنولوجي الحاصل، وبين اقتضاء حق الدولة والأفراد حال المساس بها نتيجة ممارسة هذا الحق.

وفي سبيل تحقيق ما سلف نظم المشرع مجموعة الأحكام الإجرائية في نصوص قانونية متفرقة، منها ما تعلق بجمع الاستدلالات من ضبط وتفتيش وخبرة، ومنها ما تعلق بالإجراءات الاحترازية والعقوبات التبعية اللازمة للمحافظة على الأدلة، ثم تنظيم حالات الإعفاء من العقاب والتشديد، وأخيراً تناول قواعد المسئولية الجنائية لمقدمي الخدمة التقنية، وهو ما سنتناوله تفصيلاً في المطالب التالية:

تقسيم:

سوف نقوم بتقسيم الدراسة فى هذا المبحث الى ثلاثة مطالب كما يلي:

المطلب الأول: إجراءات جمع الأدلة والاستدلالات التقنية.

المطلب الثاني: التدابير والإجراءات التحفظية والعقوبات التبعية.

المطلب الثالث: الأحكـــام العامـــة المتعلقـــة بالعقوبـــة.

المطلب الأول

إجراءات جمع الأدلة والاستدلالات التقنية

تمهيد:

لا خلاف في أن إجراءات جمع الأدلة والاستدلالات التقنية ذات طبيعة خاصة، وتحتاج لمتطلبات فنية، وخبرات معلوماتية معينة تساعد في التوصل لكشف الحقيقة، فكان من المتعين أن يعهد بهذه المهمة الحساسة والدقيقة لأشخاص يتم اختيارهم من بين أفضل العناصر الموجودة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية، والخبرة الفنية في مجال علوم التقنية، وبرمجة الشبكات، ونظم المعلومات.

ويشترط لاختيار هؤلاء الخبراء ضرورة ان يتم اختيارهم ممن تلقوا تدريباً كافياً على التعامل مع نوعيه الآثار والأدلة التي يحويها مسرح الجريمة التقنية، وتكون مهمة هؤلاء الخبراء هى مرافقه المحققين أثناء مباشرة إجراءات الاستدلال من ضبط وقبض وتفتيش وغير ذلك، إلى جانب قيامهم بفحص كل جهاز، ونقل نسخه منه على الاسطوانة الصلبة، وفحص بيانات البريد الالكتروني.

وينتهى عمل هؤلاء الخبراء بإعداد تقرير فني مفصل بما تم من إجراءات، وما توصلوا إليه من نتائج فنية يرسل إلى القاضي، أو الجهة المختصة بمباشرة التحقيق، لاتخاذ شئونها وفحص التقرير وضمه لملف التحقيقات.

من هنا فقد حرص المشرع المصري عند إصدار القانون رقم ١٧٥ لسنة ٢٠١٨ الخاص مكافحة جرائم تقنية المعلومات ولائحته التنفيذية على تنظيم إجراءات جمع الأدلة التقنية، حيث قسم هذه الإجراءات إلى ثلاثة أنواع، النوع الأول: يتعلق بإجراءات الضبط والتفتيش، والنوع الثاني: يتعلق بإجراءات الاستعانة بالخبرة الفنية أو التقنية، والنوع الثالث والأخير يتعلق بمدي الحجية القانونية أو القيمة الثبوتية للأدلة الرقمية المستخرجة من الوسائل التقنية.

تقسيم:

ولتحقيق متطلبات هذا الجانب من الدراسة سوف نقوم بتقسيم دراسة هذا المطلب إلى ثلاثة فروع، على النحو التالي:

الفرع الأول: إجراءات الضبـــــط والتفتيـــــش

الفرع الثاني: إجراءات الاستعانة بالخبـــرة الفنيـــة

الفرع الثالث: الحجية القانونية للأدلة الرقمية

الفرع الأول

إجراءات الضبـط والتفتيـش

تتميز الجرائم التقنية الناتجة عن الاستخدام أو الاستغلال غير المشروع لوسائل التقنية المعلوماتية وما ترتبه من أثار فنية معقدة بطبيعة خاصة، وتحتاج إلى متخصصين في ذات المجال يكونون على قدر من الدراية والمعرفة الفنية والقدرة على كشف غموض هذه الجرائم، وفك طلاسمها من خلال ضبط وتفتيش مرتكبيها، أو من ساعد أو سهل لارتكابها.

ففي فرنسا أسندت لفريق مكون من ١٣ شرطي مهمة القيام بالإشراف على تنفيذ المهمات الفنية التقنية، التي يعهد بها إليهم أعضاء النيابة والمحققين، وجميعهم تلقوا تدريباً متخصصاً إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بمرافقه المحققين أثناء التفتيش، حيث يقومون بفحص كل جهاز، وينقلون نسخه من الاسطوانة الصلبة، وبيانات البريد الالكتروني، ثم يقومون بعمل تقرير يرسل إلى قاضي التحقيق، أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعاده المعلومات من على الاسطوانة الصلبة، كما يمكنها قراءه الاسطوانات المرنة والصلبة والتالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءه الحاسبات المحمولة[١].

وإزاء ذلك فقد أجاز المشرع المصري في المادة الخامسة من قانون مكافحة جرائم تقنية المعلومات لوزير العدل بالاتفاق والتنسيق مع الوزير المختص[٢] منح صفة الضبطية القضائية للعاملين بالجهاز[٣] أو غيرهم ممن تحددهم جهات الأمن

---

(١) د/ صالح أحمد البربري – دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٠٠١/١١/٢٣– بحث منشور عبر شبكة الانترنت بموقع الدليل الالكتروني للقانون العربي بتاريخ ٢٠٠٦/٩/٢. (www.arablawinfo.com)

(٢) يقصد بالوزير المختص: الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات.

(٣) يقصد بالجهاز: الجهاز القومي لتنظيم الاتصالات.

القومي[١]، للقيام بمهام الضبط والتفتيش والدخول والنفاذ للبرامج والأنظمة المعلوماتية وجمع الأدلة اللازمة عن الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم.

وقد أسند المشرع المصري لجهة التحقيق المختصة مهمة تحديد المهام والاختصاصات التي يقوم بها مأموري الضبط المختص، من خلال إصدار أمر مسبب لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة إن دعت الحاجة لذلك، ومتى كان له فائدة في ظهور الحقيقة وكشف الجريمة، مع ضرورة أن يكون الأمر الصادر من جهة التحقيق في هذا الشأن مسبباً.

كما أورد المشرع في المادة السادسة[٢] من ذات القانون مجموعة الاختصاصات التي يمكن منحها لمأمور الضبط القضائي، وفي الفقرة الأخيرة من ذات المادة نظم المشرع إجراءات الطعن على الأوامر الصادرة في هذا الشأن من جهة التحقيق، حيث جعل الطعن عليها بالاستئناف أمام المحكمة الجنائية المختصة منعقدة في غرفة مشورة، وأحال في ذات الفقرة إلى قانون الإجراءات الجنائية

---

(١) يقصد جهات الأمن القومي: رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

(٢) تنص المادة (٦) من قانون التقنية المصري على أن" لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي: ١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتض. ٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط. ٣- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني.
وفي كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسببا. ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة، في المواعيد ووفقا للإجراءات المقررة بقانون الإجراءات الجنائية.

فيما يتعلق بالمواعيد والإجراءات المنظمة لذلك باعتباره الشريعة العامة للقوانين الجنائية الخاصة.

وفي ذات الصدد ذهب المشرع الكويتي أيضاً إلى تنظيم عملية اختيار مأموري الضبط القضائي وتحديد اختصاصاتهم، ولكنه لم يتوسع في هذا الأمر، وقام بمنح مأمور الضبط بعض السلطات والاختصاصات المحدودة، مغايراً لما اتخذه المشرع المصري من إجراءات ونصوص، فقد اسند المشرع الكويتي في المادة الخامسة عشر منه عملية تحديد رجال الضبط القضائي للوزير المختص الذي يحدده مجلس الوزراء[١]، عكس ما هو متبع لدي المشرع المصري الذي منح هذا الأمر لوزير العدل بالاتفاق مع الوزير المختص بالاتصالات وتكنولوجيا المعلومات.

ونعيب على المشرع الكويتي غموضه وعدم وضوح النص ودقته في تحديد المقصود بالوزير المختص[٢]، أي أنه أغفل عن عمد عدم تحديد هذا الوزير وجعل الأمر متروكاً لهوي مجلس الوزراء يختار من يشاء من غير المختصين بهذا الأمر الفني عالي التقنية في حين أن الوضع الثابت والمستقر عليه فقهاً وعملاً أن هذا الوزير يجب أن يكون هو وزير الاتصالات والمعلومات نظراً لطبيعة عمله واختصاصاته التقنية، أضف إلى ذلك أن مهمة تحديد مأموري الضبط القضائي، وبيان طبيعة أعمالهم يدخل في صميم الأعمال والاختصاصات القضائية التي يتولاها وزير العدل، مما يعني أنه كان من الواجب والمتعين على المشرع الكويتي عدم ترك أمر تحديد الوزير لهوي مجلس الوزراء والنص على إسناد هذه المهمة صراحة لوزير العدل بالتعاون مع وزير الاتصالات والمعلومات

---

(١) تنص المادة ١٥ من القانون الكويتي على أن "للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص ضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون وتحرير المخالفات عنها، وإحالتها إلى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهيلات اللازمة لهؤلاء الموظفين".

(٢) تنص المادة الأولي من قانون التقنية الكويتي على أن "في تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية، المعنى الموضح قرين كل منها : الوزير المختص: الوزير الذي يحدده مجلس الوزراء".

مثلما هو متبع لدي المشرع المصري الذي كان موفقاً في صياغة هذا الجانب الإجرائي من توزيع المهام والاختصاصات كما سلف.

ونعيب على المشرع الكويتي أيضاً بذات المادة عدم الدقة عند قيامه بتحديد مهام مأموري الضبط القضائي التي قصرها على القيام بضبط الجرائم، وتحرير المخالفات، وإحالتها إلى النيابة العامة فقط، دون أن يشير إلى أعمال التفتيش والتتبع والتحفظ على البيانات، والدخول إلي الأنظمة وقواعد البيانات،.... وغير ذلك من الاختصاصات الهامة التي تتطلب تنظيم تشريعي معين، ونعيب عليه أيضاً عدم سلامة الصياغة القانونية لعبارة تحرير المخالفات عنها والتي كان يجب أن تكون تحرير محاضر بالجرائم المرتكبة لضبط العبارة وسلامة الصياغة أضف إلى ذلك أننا أمام جريمة تقنية وليس مخالفة تستوجب الغرامة فشتان بين هذا وذاك.

وعلى النقيض من ذلك أغفل المشرع السعودي أمر تنظيم هذه الجوانب الإجرائية، حيث لم يرد بنصوص نظام المكافحة السعودي أية نصوص تفيد إسناد أعمال الضبط، والتفتيش، وجمع الاستدلال، لمأموري ضبط قضائي من الفنيين مثلما فعل سابقيه، وقصر الإشارة فقط في المادة الرابعة عشر منه على منح مهمة القيام بالإعمال الإجرائية وجمع الاستدلالات للجهات الأمنية على أن تتولي هيئة الاتصالات وتقنية المعلومات تقديم الدعم الفني لها ولجهات التحقيق والمحاكمة[1]، الأمر الذي نري أنه سيؤدي إلى التعطيل والتباطؤ والقصور في اتخاذ الإجراءات اللازمة لجمع الاستدلالات ومكافحة الجريمة، وعدم الدقة الواجبة في جمع الأدلة مما يؤدي إلى فرار المجرمين وعدم التوصل إلى الأدلة والملابسات نظراً لطبيعتها الفنية وقدرة الجناة على التخفي والهرب وإخفاء الأدلة ومعالم الجريمة بالمقارنة بمثيلتها حال ما إذا أسندت هذه المهمة إلى مأموري ضبط متخصصين

(١) تنص المادة (١٤) من نظام التقنية السعودي على أن "تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة ".

في هذه الطائفة من الجرائم المعلوماتية.

وفي المادة ٤٩ من التقنين الإماراتي منح المشرع مهمة تحديد مأموري الضبط القضائي لوزير العدل، في حين أننا نعيب عليه عدم تحديده لمهامهم واختصاصاتهم وطبيعة أعمالهم، وقصرها عمل واحد فقط هو إثبات الأفعال التي تقع بالمخالفة لأحكام القانون، مع إلزامه للسلطات المحلية بتقديم التسهيلات في ذلك[١].

خلاصة القول إذن أننا نشيد بموقف المشرع المصري في تنظيم إجراءات الضبط والتفتيش وجمع الأدلة وسلامة صياغته التشريعية، وندعو مشرعي الدول المقارنة لإعادة النظر في نصوصها التشريعات والإجرائية مع ضرورة الاقتضاء بما اتبعه المشرع المصري في هذا الخصوص على النحو المتقدم.

(١) وتنص المادة ٤٩ من القانون الإماراتي على أن "يكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفة مأموري الضبط القضائي في إثبات الأفعال التي تقع بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم".

الفرع الثاني

إجراءات الاستعانة بالخبـــرة الفنيـــة

تلعب الخبرة الفنية دوراً هاماً في عملية الإثبات، وكشف طلاسم الجريمة المعقدة حينما لا تكون سلطات الاستدلال والتحقيق والمحاكمة على دراية فنية كافية بالأمور المعقدة المتعلقة بالجريمة والتي لا يمكن للعقل البشري والنشاط الإنساني العادي التوصل إليها، الأمر الذي يتطلب بالضرورة الاستعانة بأهل الخبرة والدراية الفنية لكشف حقيقة وملابسات الجريمة والظروف المحيطة بها .

ومما لا شك فيه أن الجرائم المرتبطة بتقنية المعلومات باتت تفرض وجودها، وتنتشر بشكل ملحوظ، فكان من الضروري الاستعانة بخبراء فنيين لمعاونة رجال الضبط والتحقيق والمحاكمة، وتقديم المشورة الفنية لهم حال طلب ذلك، ويقصد بالخبرة وفقاً لأحكام قانون تقنية المعلومات المصري، كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في مجالات تقنية المعلومات(١).

وقد أحسن المشرع المصري صنعاً بتناوله النص صراحة في الفقرة الأولي من المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات على ضرورة الاستعانة بخبراء فنيين في عملية البحث والتحري وجمع الاستدلالات(٢).

وتناول في الفقرة الثانية من ذات المادة تنظيم عمل الخبراء الفنيين، وبيان التزاماتهم وواجباتهم وحقوقهم، وضوابط مسائلتهم تأديبياً مع الإحالة إلى مجموعة القواعد والأحكام التقليدية المتعارف عليها الخاصة بتنظيم أعمال الخبرة أمام

---

(١) يراجع نص المادة الأولي من قانون تقنية المعلومات المصري المتعلقة ببيان المعاني والمصطلحات.

(٢) نصت الفقرة الأولي من المادة العاشرة على أن "ينشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به".

القضاء[١].

ووعياً من المشرع المصري بأهمية دور الخبراء الفنيين في مجال تقنية المعلومات فقد تناول في اللائحة التنفيذية للقانون الصادرة بموجب قرار مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠[٢] طرق وشروط اختيار الخبراء وتنظيم عملهم وضوابط القيد في كل سجل من السجلين المشار إليهما في القانون وذلك على النحو التالي:

أولاً: قواعد وشروط قيد الخبراء في السجل الأول الخاص بالفنيين والتقنيين العاملين بالجهاز[٣]:

١- أن يكون حاصلاً على مؤهل علمي أو فني أو تقني يتناسب ومجال الخبرة.
٢- أن يكون قد أمضي عام على الأقل في عمله بالجهاز.
٣- أن يجتاز الاختبارات الفنية التي يجريها الجهاز للمتقدم.

ثانياً: قواعد وشروط قيد الخبراء في السجل الثاني الخاص بالفنيين والتقنيين من غير العاملين بالجهاز[٤]:

١- أن يكون مصرياً متمتعاً بالأهلية المدنية الكاملة، ويجوز قيد الأجنبي بشرط أن يتعهد كتابةً بخضوعه للقوانين المصرية.
٢- أن يكون محمود السيرة حسن السمعة .

---

(١) نصت الفقرة الثانية من المادة العاشرة على أن ".... وتطبق على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء. واستثناء من تلك القواعد، تسري على الخبراء المقيدين بالسجل الثاني القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وجد. وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد في كل من السجلين".

(٢) منشور بالجريدة الرسمية في العدد ٣٥ تابع (ج) – بتاريخ ٢٧ أغسطس سنة ٢٠٢٠.

(٣) يراجع نص المادة (٤) من اللائحة التنفيذية للقانون سالفة البيان.

(٤) يراجع نص المادة (٥) من اللائحة التنفيذية للقانون سالفة البيان.

٣- ألا يكون قد سبق الحكم عليه بحكم نهائي بالإدانة في جريمة مخلة بالشرف.

٤- أن يكون لديه سيرة ذاتية تتضمن خبرة عملية مناسبة .

٥- موافقة الجهات المعنية من جهات الأمن القومي على القيد بالسجل.

وفي حالة إذا ما تخلف أي شرط من الشروط السابقة في الخبير يؤدي ذلك إلى شطبه من السجل بقرار من الجهاز .

ثالثاً: إجراءات قيد الخبراء من غير الفنيين أو التقنيين العاملين بالجهاز[١]:

حددت الفقرة الأولي من المادة الثامنة من ذات اللائحة التنفيذية إجراءات قيد الخبراء من غير العاملين بالجهاز لتكون علي النحو التالي:

١-أن يتقدم من يرغب في قيد أسمه في السجل الثاني للخبراء بطلب كتابي.

٢-أن يقدم هذا الطلب كتابةً للرئيس التنفيذي للجهاز .

٣-أن يوضح بهذا الطلب التخصص الذي يرغب العمل فيه كخبير.

٤-أن يرفق بهذا الطلب صور الشهادات والمستندات المؤيدة لطلبه.

وحال تحقق هذه الشروط في طالب القيد بسجل الخبراء من غير الفنيين العاملين بالجهاز، يجب على الجهاز أن يبت في الطلب المقدم منه خلال ستون يوماً من تاريخ تقديمه، ويعتبر عدم الرد خلال هذه المدة رفضاً ضمنياً لطلبه، وفي هذه الحالة أو حالة الرفض الصريح يحق للمتقدم التظلم بالإجراءات المقررة قانوناً[٢].

وهذا وقد بينت اللائحة التنفيذية للقانون في المادة السادسة منها طبيعة عمل

---

(١) يراجع نص الفقرة الأولي المادة (٨) من اللائحة التنفيذية للقانون سالفة البيان .

(٢) تنص الفقرة الثانية من المادة (٨) من اللائحة التنفيذية للقانون على أن "ويمكن للجهاز أن يطلب منه خلال ثلاثون يوماً من تاريخ تقديم الطلب معلومات إضافية قبل الفصل في الطلب، ويعتبر عدم الرد على الطلب لمدة ستين يوماً من تاريخ تقديمه رفضاً له، وفي حال رفض الجهاز الطلب يحق للمتقدم التظلم بالإجراءات المقررة قانوناً".

الخبراء الفنيين أو التقنيين وقصرها على تنفيذ المهام الفنية والتقنية التي يتم تكليفهم بها من جهات التحقيق أو الجهات القضائية المختصة أو من الجهات المعنية بمكافحة جرائم تقنية المعلومات بشأن الجرائم موضوع هذا القانون[١].

وأخيراً نشيد بمسلك المشرع المصري، وحرصه على إسناد بعض الأعمال الفنية الدقيقة لخبراء تقنيين على دراية كافية بشئون وأنظمة تكنولوجيا تقنية المعلومات، يتم اختيارهم وفق ضوابط وشروط معينة، ليكونوا عوناً وسنداً لجهات التحقيق والمحاكمة في مكافحة الجريمة التقنية وضبط أدلتها، وهو مسلك محمود لم نري له مثيل بالتشريعات المقارنة التي لم تتناولها لا من قريب أو من بعيد.

وعلى الرغم من ذلك نعيب على المشرع المصري نصه على الإحالة إلى القواعد التقليدية المنظمة لعمل الخبراء والمعمول بها أمام القضاء، خاصة أن عمل الخبير التقني تختلف تماماً عن عمل الخبراء العاديين التقليديين، فكان من المعين عليه أن يضع نصوص صريحة وواضحة لتنظيم عمل الخبراء التقنيين وتحديد اختصاصاتهم صراحة بصلب هذا القانون أو اللائحة دون الإحالة إلى نصوص تقليدية قد لا تتناسب مع عمل الخبراء التقنيين والبعد عن العمومية في النص.

(١) يراجع نص المادة (٦) من اللائحة التنفيذية للقانون سالفة البيان .

الفرع الثالث

الحجية القانونية للأدلة الرقمية

عرفت المادة الأولي من قانون مكافحة جرائم تقنية المعلومات الدليل الرقمي بأنه أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة(١).

وبموجب نص المادة الحادية عشر من القانون اعترف المشرع المصري لهذه الأدلة الرقمية المستمد من وسائل التقنية الحديثة بقيمتها الثبوتية، ومنحها ذات القيمة القانونية والحجية الثبوتية الممنوحة للأدلة الجنائية المادية في الإثبات الجنائي، المقررة بموجب قانون الإجراءات الجنائية المصري ١٥٠ لسنة ١٩٥٠ وتعديلاته، وقواعد الإثبات المتعارف عليها فقهاً وقضاءً وقانوناً.

وفي حقيقة الأمر هذه الأدلة التقنية هي أدلة معقدة وتحتاج لقبولها في عملية الإثبات ضرورة توافر شروط ومواصفات معينة مغايرة للأدلة المادية التقليدية، وقد تنبه المشرع المصري لهذا الأمر الهام، واشترط في الفقرة الأخيرة من ذات المادة سالفة البيان لقبول هذه الأدلة التقنية في الإثبات ضرورة أن يتوافر بها بعض الشروط والضوابط والمواصفات الفنية المعينة التي تمنحها هذه القوة الثبوتية، وأحال بشأنها إلى نصوص اللائحة التنفيذية لقانون مكافحة جرائم التقنية المعلوماتية المصري(٢).

هذا وقد بينت اللائحة التنفيذية للقانون الصادرة بموجب قرار مجلس الوزراء

---

(١) يراجع نص المادة الأولي من قانون تقنية المعلومات المصري الصادر في شأن مكافحة جرائم التقنية.

(٢) تنص المادة الحادية عشر من ذات القانون على أن " يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتى أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

رقم ١٦٩٩ لسنة ٢٠٢٠ أهم الشروط والضوابط الواجب توافرها في الدليل التقني لقبوله والاعتراف بحجيته وقيمته الثبوتية، إضافة لما تطلبته من إجراءات معينة ولازمة لتقديم هذا الدليل أمام الجهات المختصة، وذلك على النحو التالي:

أولاً: بالنسبة للشروط والمواصفات الواجب توافرها في الدليل التقني:

فقد حددت المادة التاسعة من اللائحة التنفيذية المشار إليها هذه الشروط والضوابط والمواصفات بنصها على أن " تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي إذا توافرت فيها الشروط والضوابط الآتية:

١- أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة لمعلومات أو البرامج أو الدعامات الالكترونية وغيرها. ومنها على الأخص تقنية Write Blocker, Digital Images Hash, وغيرها من التقنيات المماثلة .

٢- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، وفقاً لنطاق قرار جهة التحقيق أو المحكمة المختصة .

٣- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، وعلى أن يبين في محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به .

٤- في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على

الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص أو التحليل.

٥- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته .

ثانياً: بالنسبة لإجراءات تقديم الدليل التقني من توثيق وتوصيف واعتماد:

حددت المادة العاشرة من ذات اللائحة هذه الإجراءات بنصها على أن " يتم توصيف وتوثيق الدليل الرقمي من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأي وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات التالية على كل منها:

١- تاريخ ووقت الطباعة والتصوير .
٢- اسم وتوقيع الشخص الذي قام بالطباعة والتصوير .
٣- اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به .
٤- اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ .
٥- البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط .
٦- بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة .

وبذلك يكون المشرع قد أقر صراحة بقيمة وحجية الأدلة الرقمية المستخرجة من الوسائل والأنظمة المعلوماتية التقنية، وأعترف بقوتها التدليليه في مجال الإثبات الجنائي وهو بذلك يكون قد أحسن صنعاً من غيره في مواكبة التطورات الحاصلة في مجال تكنولوجيا المعلومات ووسائل التقنية الحديثة وإدخالها في الأنظمة التشريعية والقضائية، مسايراً ما ذهبت إليه أغلب التشريعات الأوروبية والأجنبية في هذا الشأن والتي من بينها، التشريع الانجليزي الصادر عام ١٩٨٤ المعمول به اعتباراً من ١٩٨٦ والمتعلق بالإثبات، وقانون إساءة استخدام

الحاسوب عام ١٩٩٠ اللذين حويا تنظيماً محدداً لمسألة قبول مخرجات الانترنت والحاسب الآلي كأدلة إثبات في المواد الجنائية[١]، وكذا التشريع الأمريكي المتعلق بالإثبات وقبول الأدلة والمخرجات الالكترونية في عملية الإثبات، والاعتراف بقيمتها وقوتها التدليلية[٢].

ويكمن السبب الرئيسي وراء هذا الاعتراف بالقيمة الثبوتية للأدلة التقنية الرقمية وإقرار حجيتها في مجال الإثبات الجنائي من وجهة نظر رجال الفقه القانوني يرجع إلى أن هذه الأدلة أدلة مُحكمة بقواعد علمية وحسابية دقيقة وقاطعة لا تقبل التأويل أو الشك، بالإضافة إلى وضوحها ودقتها في إثبات الصلة بين الجاني والمجني عليه أو بين الجاني والسلوك غير المشروع، مما يقوي من يقينية تلك الأدلة والمستخرجات لدي محكمة الموضوع[٣]، وكنا نأمل من المشرع المصري أن يأخذ في الاعتبار عند النص على هذه الشروط والمواصفات الواردة باللائحة التنفيذية مجموعة الشروط العامة المتفق عليها في المجتمع الدولي وأغلب التشريعات الدولية لقبول حجية الدليل الالكتروني[٤].

وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة التي تكون

---

(١) وقد ركزا هاذين القانونين بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه والتي تزود بشهادة شفوية تكون مقبولة والتي يتم تقديرها من قبل المحكمة المختصة– راجع تفصيلاً: د/ سعيد عبد اللطيف حسن– إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت– دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩، ص١٩٤ وما بعدها.

(٢) د/ هلالي عبد اللاه أحمد– تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى، مطبعة دار النهضة العربية، الطبعة الأولي، القاهرة، ١٩٩٧، ص٥٣.

(٣) د/ ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، المغرب، العدد٣١، رجب١٤٢٧، ص١٣٢.

(٤) ومن هذه الشروط ضرورة أن تكون هذه الأدلة مشروعة، أن يتم طرحها وعرضها للمناقشة، أن تتمتع باليقينية، مشار إلى هذه الشروط والضوابط في رسالتنا للدكتوراه بعنوان، دور الانترنت في الإثبات أمام القاضي الجنائي والإداري، دراسة مقارنة، كلية الحقوق، جامعة عين شمس، ٢٠١٧، ص٦٥٥ وما بعدها.

لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي[١]، كما قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان (MC Mullen)، بأنه يشترط لكي تكون سجلات الحاسوب مقبولة بوصفها نسخاً حقيقية من السجلات الإلكترونية، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفاً للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كافٍ[٢].

وعلى النقيض من ذلك نجد مشرعي بعض الدول المقارنة يقفوا مكتوفي الأيدي، فلم نجد في التشريعات العربية المقارنة أية نصوص أو إشارات صريحة تعترف بقيمة وحجية الأدلة المستخرجة من وسائل التقنية أسوة بالمشرع المصري وأغلب التشريعات الأوروبية، وهو ما يدعونا إلى ضرورة حس مشرعي هذه الدول نحو الإسراع لوضع أسس وآليات وضوابط لقبول هذه الأدلة التقنية في مجال إثبات الجريمة المعلوماتية والاقتضاء بما فعله المشرع المصري مسايرة للتطورات الحاصلة في هذا الشأن .

---

(١) د/ هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، الطبعة الأولي، دار النهضة العربية، القاهرة، ١٩٩٧، ص٤٢ وما بعدها. د/علي حسن الطوالبه، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة، بحث منشور عبر الانترنت، مركز الإعلام الأمني، البحرين، ٢٠٠٩، ص١٧.

(٢) د/هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص٥٥ وما بعدها. د/علي حسن الطوالبه، مشروعية الدليل الالكتروني، المرجع السابق، ص١٨.

المطلب الثاني

التدابير والإجراءات التحفظية والعقوبات التبعية

تمهيد:

لم يقف الأمر بالمشرع المصري عند هذا الحد من إجراءات الاستدلال واجبة الإتباع حال مباشرة التحقيق والمحاكمة مع الجاني في الجرائم المعلوماتية، بل لقد نظم المشرع مجموعة أخرى من الإجراءات التي نطلق عليها مجموعة الإجراءات التحفظية السابقة على التحقيق أو التي تتم أثناء مباشرة إجراءاته، وهذه الإجراءات تتشابه إلى حد ما بالإجراءات الاحترازية المقررة بقانون العقوبات المصري.

ومن أهم الإجراءات التي قررها المشرع بقانون مكافحة جرائم تقنية المعلومات حجب المواقع التي استخدمت أو ارتكبت الجريمة من خلالها، التحفظ على الجاني ومنعه من السفر للحفاظ على الأدلة ومنع هروب الجناة وتتبعهم، إضافة إلى أنه أجاز للمحكمة أن تقضي ببعض العقوبات التبعية إلى جانب العقوبة الأصلية.

وسوف نتناول هاذين الجانبين من الإجراءات في المطلب الماثل من خلال تقسيمه إلى فرعين، نخصص الفرع الأول لدراسة مجموعة الإجراءات التحفظية، والفرع الثاني لدراسة العقوبات التبعية أو التكميلية، وذلك على النحو التالي.

تقسيم:

سوف نقوم بتقسيم هذا المطلب الى فرعين كما يلي:

الفرع الأول: التدابير والإجراءات التحفظية.

الفرع الثاني: العقوبات التبعية أو التكميلية.

الفرع الأول

التدابير والإجراءات التحفظية

تمهيد:

تنقسم مجموعة الإجراءات التحفظية الواردة بقانون تقنية المعلومات المصري إلى نوعين من الإجراءات، أولهما حجب المواقع الإلكترونية التي استخدمت في ارتكاب الجريمة أو كانت مسرحاً لها، والإجراء الأخر هو المنع من السفر وترقب الوصول، واللذين سوف نتناولهما من خلال تقسيم هذا الفرع إلى غصنين، نخصص أولهما لدراسة قرار الحجب والتظلم منه، والثاني لقرار المنع من السفر.

تقسيم:

سوف نقوم بتقسيم الدراسة فى هذا الفرع الى غصنين كما يلي:

الغصن الأول: حجب المواقع الالكترونية والتظلم منها.

الغصن الثاني: المنع من السفر وترقب الوصول.

الغصن الأول

حجب المواقع الإلكترونية والتظلم منها

أولاً: حجب المواقع الإلكترونية:

نظم المشرع المصري في الفقرة الأولي من المادة السابعة من القانون إجراءات وضوابط حجب المواقع الإلكترونية بهدف حماية القيم والأخلاق المجتمعية وحقوق الأفراد وخصوصيتهم، وقد أوكل المشرع لجهة التحقيق المختصة مهمة إصدار قرار الحجب للمواقع المخالفة، بقوله أن لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدا للأمن القومي

أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا[١].

ولم يترك المشرع قرار الحجب في يد جهة التحقيق مستقلة دون رقابة أو إشراف، بل لقد ألزمها بضرورة أن تقوم بعرض أمر الحجب على المحكمة المختصة منعقدة في غرفة مشورة خلال أربعة وعشرين ساعة، مع ضرورة قيامها بتحرير مذكرة برأيها والأسباب التي دعتها لاتخاذ ذلك الإجراء بإصدار أمر الحجب، وتتولي هذه المحكمة مهمة التعقيب عليه وتصدر قرارها في الأمر مسببا إما بالقبول أو بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرض الأمر عليها[٢].

أما وإن كان هناك خطر حال أو ضرر وشيك الوقوع يتطلب الإسراع في اتخاذ إجراءات الحجب، ففي هذه الحالة يكون الاختصاص باتخاذ إجراءات الحجب لجهات التحري والضبط عن طريق إبلاغ الجهاز بذلك، ليقوم على الفور بدوره بإخطار مقدم الخدمة بالحجب المؤقت للموقع أو المحتوى أو المواقع أو

---

(١) وإعمالا لذلك فقد أصدر النائب العام المصري عدة قرارات تتعلق بهذا الشأن، منها القرار الصادر عام ٢٠١٨ بتكليف الجهاز القومي لتنظيم الاتصالات باتخاذ ما يلزم من إجراءات لحجب المواقع التي تبث الألعاب الالكترونية على شبكة الانترنت ومنها ما يسمي " الحوت الأزرق" وغيرها باعتبار أن هذه الألعاب ذات خطورة كونها تستهدف صغار السن ويترتب عليها إيذاء ما، قد يصل الأمر أحيانا للانتحار وارتكاب جرائم القتل وهو أمر يمس امن وسلامة قطاعا عريضا من الأسرة المصرية وما يعد من قبيل الأمن القومي، يراجع قرار معالي المستشار النائب العام الصادر بتاريخ ٢٠١٨/٤/٢١. ومنها أيضاً القرار الصادر عام ٢٠١٩ بتكليف وزارة الاتصالات وتكنولوجيا المعلومات باتخاذ ما يلزم من إجراءات تقنية لحجب المواقع التي تقوم ببث أي صور أو مواد مسجلة أو مقاطع فيلمية منافية للآداب (إباحية وجنسية) على خليفة، والصادر بتاريخ ٢٠١٩/٢/١٢ بمناسبة التحقيق في القضيتين رقمي ٦٤٢٧ لسنة ٢٠١٩، ٨٢٤٢ لسنة ٢٠١٩ جنح أول مدينة نصر.

(٢) تنص الفقرة الثانية من ذات المادة على أن" وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة خلال أربع وعشرين ساعة مشفوعا بمذكرة برأيها. وتصدر المحكمة قرارها في الأمر مسببا إما بالقبول أو بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها".

الروابط المذكورة في الفقرة الأولى من هذه المادة وفقا لأحكامها، مع ضرورة أن يلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه[١].

وقد نظمت تلك المادة الإجراءات واجبه الإتباع حال صدور أمر الحجب من الجهة المختصة والمحددة بالفقرة الثالثة من المادة السابعة بحيث يجب على هذه الجهات أن تثبت ما قامت به من إجراءات في محضر رسمي يعرض على جهات التحقيق خلال ثمان وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز والمنوه عنه بعالية، وتتبع في هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة، والتي تتمثل في العرض على المحكمة المختصة خلال أربعة وعشرين ساعة لتتخذ قراراها في هذا الشأن إما بالتأييد أو بوقف ما تم من إجراءات، وإذا لم يعرض هذا المحضر المشار إليه في الموعد المحدد، وعلى النحو المبين بعالية، يعد الحجب الذي تم كأن لم يكن[٢].

والجدير بالذكر أن المشرع حدد أساليب وطرق انتهاء العمل بقرار الحجب وتعديله وبيان أسبابه بقولها يتم رفع الحجب وانتهاء العمل به أو تعديل نطاقه بقرار من محكمة الموضع المختصة من تلقاء نفسها ووفق ما تراه من أسباب، أو بناء على طلب جهة التحقيق أو الجهاز أو ذوي الشأن، وفي جميع الأحوال، يسقط هذا القرار بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة[٣].

وبمطالعة نصوص التشريعات المقارنة الصادرة في شأن تقنية المعلومات، نجد أن اغلبها أغفل تناول إجراء حجب المواقع نهائياً، وحل محله الإغلاق، ومن

---

(١) تنص الفقرة الثالثة منها على أن" ويجوز في حالة الاستعجال لوجود خطر حال، أو ضرر وشيك الوقوع، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة في الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه".

(٢) يراجع نص الفقرتين الرابعة والخامسة من المادة السابعة من القانون.

(٣) يراجع الفقرتين السادسة والسابعة من المادة السابعة سالفة البيان.

بين هذه التشريعات، التشريع الكويتي[١]، والسعودي[٢]، والإماراتي[٣]، حينما نصت جميعها بجواز الحكم إغلاق الموقع أو مكان تقديم الخدمة سواء أكان إغلاق نهائي أم مؤقت متى كان ذلك مصدراً لارتكاب الجريمة أو تمت بعلم مالكها.

أضف إلى ذلك أنهم وإن أجازوا الحكم بالإغلاق إلا أنهم قصروا استخدام هذه السلطة على محكمة الموضوع فقط دون غيرها على الرغم من أهميه هذا الإجراء خلال مرحلتي جمع الاستدلال والتحقيق، وذلك بقولها " جواز الحكم بإغلاق الموقع.." خاصة وأنه من المتفق عليه أن الحكم لا يصدر إلا من محكمة لا من جهة تحقيق أو استدلال، الأمر الذي يترتب عليه استمرار وقوع الجريمة، أو الانتهاكات طوال فترة التحقيق، أو الاستدلال طالما لم يتم إيقاف البث أو الحجب، وانتظار صدوره من محكمة الموضوع التي قد لا تري وجوباً لصدوره؛ كما أنه يؤخذ عليهم أيضاً عدم تحديد المدة التي يجب أن يصدر خلالها الحكم بهذا الإغلاق، وتركوا الأمر طليقاً دون قيد للسلطة التقديرية لمحكمة الموضوع دون

---

(١) تنص المادة (١٣) من التشريع الكويتي على أنه" يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي أرتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية أو بحق المضرور في التعويض المناسب. ويكون الحكم بإغلاق المحل أو الموقع وجوبيا إذا تكرر ارتكاب أيا من هذه الجرائم بعلم مالكها.

(٢) تنص المادة (١٣) من التشريع السعودي على أنه" مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

(٣) تنص المادة (١٣) من التشريع السعودي على أنه" مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة .

إلزام عليها بموعد محدد يجب أن يصدر خلاله حكم الإغلاق.

ثانياً: إجراءات التظلم من قرار الحجب:

تناولت المادة الثامنة من ذات القانون تنظيم إجراءات التظلم من قرار الحجب سواء وقع التظلم على قرار الحجب ذاته أو على إجراءات تنفيذه، كما لم يقتصر حق التظلم على المتهم بالجريمة فقط، بل لقد منح هذا الحق لكل ذي شأن أو صاحب مصلحة في ذلك سواء أكان المتهم بالجريمة التقنية أو النيابة العامة أو غيرهما ممن له مصلحة، على النحو التالي[١] :

أ- صاحب الحق في تقديم التظلم:

نصت الفقرة الأولي من المادة الثامنة على أن يكون الحق في التظلم من قرار الحجب لكل من صدر ضده قرار قضائي من المنصوص عليها في المادة (٧) من هذا القانون، وللنيابة العامة ولجهة التحقيق المختصة ولكل ذي شأن.

ب- مواعيد تقديم التظلم والفصل فيه :

يجب أن يقدم التظلم وفقاً لنص المادة السابعة بعد انقضاء سبعة أيام من تاريخ صدور الأمر بالحجب أو من تاريخ تنفيذه بحسب الأحوال، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويجب على هذه المحكمة أن تفصل في التظلم المقدم إليها خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به لدي كتاب المحكمة.

---

(١) تنص المادة الثامنة من التشريع المصري على أنه" لكل من صدر ضده قرار قضائي من المنصوص عليها في المادة (٧) من هذا القانون، وللنيابة العامة ولجهة التحقيق المختصة ولكل ذي شأن، أن يتظلم منه أو من إجراءات تنفيذه أمام محكمة الجنايات المختصة بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

وفي جميع الأحوال، يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز وكل ذي شأن، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به.

ج- الجهة المختصة ببحث التظلم :

لقد حدد المشرع المصري في الفقرة الثانية من المادة السابعة سالفة البيان الجهة المختصة ببحث وقبول التظلم المقدم إليها وهي محكمة الجنايات المختصة.

د- إجراءات تقديم التظلم :

يتم تقديم التظلم وفقاً للفقرة الأخيرة من المادة السابعة بموجب تقرير يودع لدي قلم كتاب محكمة الجنايات المختصة، ويتولي رئيس المحكمة تحدد جلسة لنظر هذا التظلم، مع ضرورة أن يتم إعلان كل من المتظلم والجهاز وكل ذي شأن بتاريخ هذه الجلسة.

الغصن الثاني

المنع من السفر وترقب الوصول

الأصل هو حرية الإنسان في التنقل والإقامة كيفما يشاء، وهو يعد من أهم الحقوق والحريات الإنسانية التي تناولتها كافة الاتفاقيات والمعاهدات الدولية بالتنظيم[1]، وكفلتها أغلب الدساتير والتشريعات الوطنية والعالمية، فهذا الحق يترتب علي انتهاكه إهدار العديد من الحقوق الإنسانية الأخرى، مثل حق الإنسان في التعايش والعلاج والعمل والتعليم وممارسة الشعار الدينية والتواصل الاجتماعي .

---

(١) **منها الإعلان العالمي لحقوق الإنسان في مادته رقم (١٣) التي تنص على أن** " ١- لكل فرد حق في حرية التنقل وفي اختيار محل إقامته داخل حدود الدولة . ٢ -لكل فرد حق في مغادرة أي بلد بما في ذلك بلده، وفي العودة إلى بلدة ". **ومنها أيضاً ما جاء من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي صادقت عليه مصر في ١٤ يناير ١٩٨٢، والذي نص في المادة (١٢) على أن** " ١- لكل فرد يوجد على نحو قانوني داخل أقليم دولة ما حق حرية التنقل فيه وحرية اختيار مكان إقامته. ٢- لكل فرد حرية مغادرة أي بلد بما في ذلك بلده. ٣- لا يجوز تقييد الحقوق المذكورة أعلاه بأية قيود غير تلك التي ينص عليها القانون، وتكون ضرورية لحماية الأمن القومي أو النظام العام، أو الصحة العامة، أو الآداب العامة، أو حقوق الآخرين وحرياتهم، وتكون متمشية مع الحقوق الأخرى المعترف بها في هذا العهد. ٤- لا يجوز حرمان أحد تعسفاً من حق الدخول إلى بلده".

ومما لا شك فيه أن حياة الإنسان لا تستقيم ولا تكون طبيعية إذا كانت هناك قيود تحد من حركته وتنقله بشكل عام أو منعه من السفر، فهذا المنع أو القيد يشبه إلى حد كبير الاعتقال والسجن، وأمام أهمية هذا الإجراء وما يترتب عليها من خطورة وأضرار قد يتعرض لها الإنسان جراء انتهاك هذا الحق بحرمانه من السفر وتقييد حريته، كان لابد للمشرع أن ينبري في الاهتمام بتنظيم إجراءات إصدار قرار المنع من السفر وبيان حالاته، والسلطة المختصة بإصداره، وحظر إصداره إلا في أضيق حدود ووفق ضوابط ومعايير معينة إن استلزم الأمر ذلك.

وإلى جانب هذا الحق الفردي هناك حق أكبر وأعم يجب أخذه في الاعتبار والمحافظة على تحقيقه، هو حق المجتمع في مكافحة الجريمة، وضبط المجرمين، والحفاظ على الأدلة من التلف أو العبث، والعمل على حظر فرار المجرمين وهروبهم خارج البلاد.

وانطلاقاً من ذلك فقد بادر المشرع إلى الاهتمام بهاذين الحقين والمحافظة عليهما، وتحقيق نوع من التوازن بين حقوق الإنسان الخاصة واخصها حق الإنسان في التنقل بحرية دون قيد أو تتبع أو مراقبة، وحقوق المجتمع العامة في مكافحة الجريمة وضبط المجرمين قبل هروبهم وتحقيق أدلة الجريمة، وفي هذا السياق أكدت المحكمة الدستورية العليا في أحدث أحكامها[١] على أن حرية الانتقال تنخرط من مصاف الحريات العامة، وتقييدها يتعين دائماً أن يكون بمقتضي مشروع، وتقييدها دون مسوغ مشروع يجرد الحرية الشخصية من بعض خصائصها، ويقوض صحيح بنيانها.

ولقد احتفت الدساتير المصرية جميعها بالحقوق المتصلة بالحق في التنقل، فنصت على حظر ألزام المواطنين الإقامة في مكان معين أو منعه من الإقامة في جهة معينة، إلا في الأحوال التي يبينها القانون، كما حظرت إبعاد المواطنين عن البلاد أو حرمانهم من العودة إليها، وأكدت على حق المواطن في الهجرة الدائمة

(١) حكم المحكمة الدستورية العليا في القضية رقم ٤٠ لسنة ٣٧ ق " تنازع" – جلسة ١٣ يونيو ٢٠١٥ .

أو المؤقتة، واعتبارا من تاريخ العمل بالدستور المعدل الصادر في يناير ٢٠١٤ لا يجوز منع مواطن من مغادرة الأراضي المصرية إلا بأمر قضائي مسبب، ولمدة محددة وفي الأحوال التي يبينها القانون(١).

وقد تكللت جهود المشرع المصري بالنجاح، تحقيقاً لما تقدم وخلق جو من العدالة التشريعية، وكان أخر هذه الجهود وأهمها قانون مكافحة جرائم تنقية المعلومات، والذي بادر من خلاله إلى تفعيل نص الفقرة الأخيرة من المادة ٦٢ من الدستور والعمل على تنظيم هذا الإجراء الاحترازي- المنع من السفر- فيما يتعلق بجرائم تقنية المعلومات، من خلال ما أورده في المادة التاسعة المشار إليه بعالية(٢)، والتي أسند بمقتضاها مهمة إصدار هذا الأمر أو القرار- المنع من السفر- للنائب العام أو من يفوضه من المحامين العموم الأول لنيابات الاستئناف، وكذا لجهات التحقيق المختصة، بشرط أن تكون هناك حالة من حالات الضرورة أو عند وجود أدلة كافية على جدية الاتهام في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون أو الشروع في ارتكابها.

- **إجراءات التظلم من قرار المنع من السفر(٣):**

---

(١) تواترت كافة الدساتير المصرية على الاهتمام بهذا بحق الإنسان في التنقل، وعدم تقييده أو منعه من السفر وصولاً إلى الدستور الحالي لعام ٢٠١٤ والذي نص في المادة ٦٢ منه على أن "حرية التنقل والإقامة والهجرة مكفولة، ولا يجوز إبعاد أي مواطن عن إقليم الدولة، ولا منعه من العودة إليه، ولا يكون منعه من مغادرة إقليم الدولة، أو فرض الإقامة الجبرية عليه، أو حظر الإقامة في جهة معينة عليه، إلا بأمر قضائي مسبب ، ولمدة محددة، وفي الأحوال المبينة في القانون" .

(٢) تنص الفقرة الأولي من المادة التاسعة على أنه " يجوز للنائب العام أو من يفوضه من المحامين العموم الأول بنيابات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة أو عند وجود أدلة كافية على جدية الاتهام في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون أو الشروع في ارتكابها، أن يأمر بمنع المتهم من السفر خارج البلاد، أو بوضع اسمه على قوائم ترقب الوصول، بأمر مسبب لمدة محددة.

(٣) تنص الفقرة الثانية من المادة التاسعة على أنه " ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة، خلال خمسة عشر يوما من تاريخ علمه به، فإذا رفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم. ويكون التظلم

ولم يقف الأمر بالمشرع المصري عند هذا الحد من تنظيم إجراءات إصدار أمر المنع من السفر فقط، بل توالت جهوده التنظيمية وكان من بينها وضع مجموعة من الضوابط والإجراءات التي تتضمن تنظيم الإجراءات اللاحقة على إصدار الأمر بالمنع، من أهمها إجراءات التظلم منه، حيث أتاح المشرع في الفقرة الثانية من ذات المادة لمن صدر ضده أمر بالمنع من السفر الحق في أن يبادر بتقديم تظلم إلى محكمة الجنايات المختصة خلال خمسة عشر يوما من تاريخ علمه بقرار المنع من السفر، بموجب تقرير يودع قلم كتاب المحكمة، ويجب على رئيس المحكمة أن يبادر إلى تحديد جلسة لنظر هذا التظلم، وإعلان كل من النيابة العامة والمتظلم بهذه الجلسة.

وقد ألزم المشرع المحكمة المختصة بضرورة أن تفصل في هذا التظلم خلال مدة لا تجاوز خمسة عشر يوما من تاريخ التقرير به، بحكم مُسبب بعد سماع أقوال كل من المتظلم والنيابة العامة أو جهة التحقيق حسب الأحوال، ولها في سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها في هذا الشأن.

أما في حالة أن يتم رفض التظلم المقدم من المتظلم، فيكون له الحق في أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفضه.

- **حالات وطرق انتهاء قرار المنع من السفر**[1]:

وفي جميع الأحوال ينتهي قرار المنع من السفر وفقاً لأحكام الفقرة الأخيرة

بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز خمسة عشر يوما من تاريخ التقرير به، بحكم مُسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق حسب الأحوال، ولها في سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها في هذا الشأن.

(١) تنص الفقرة الأخيرة من المادة التاسعة على أنه " ويجوز للنيابة العامة وجهات التحقيق المختصة في كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة لذلك. وفي جميع الأحوال ينتهي المنع من السفر بمرور سنة من تاريخ صدور الأمر، أو بصدور قرار بألا وجه لإقامة الدعوى الجنائية، أو بصدور قرار نهائي فيها بالبراءة، أيهما أقرب.

المادة التاسعة بإحدى الطرق أو الحالات الآتية :

١- عدول الجهة المختصة عن قرار الصادر منها بالمنع في أي وقت تشاء.
٢- تعديل القرار برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة لذلك.
٣- مرور سنة من تاريخ صدور قرار المنع من السفر.
٤- أن يصدر قرار بألا وجه لإقامة الدعوى الجنائية.
٥- أن يصدر قرار نهائي بالبراءة.

وأخيراً نشيد بجهود المشرع المصري في هذا الشأن، فقد أحسن صنعاً بتبنيه هذا الإجراء ضمن نصوص قانون مكافحة جرائم تقنية المعلومات بالمقارنة بغيره من تشريعات الدول المقارنة، التي جاءت جميعها خلواً من النص على مثل هذا الإجراء الاحترازي التحقيقى .

الفرع الثاني

العقـوبات التبعيــة أو التكميليـة

تأتى العقوبات التبعية في مرحلة المحاكمة، وقد تناول المشرع المصري النص على هذه العقوبة في المادتين ٣٨، ٣٩ من ذات القانون، حيث أوجب المشرع على المحكمة في حال الحكم بالإدانة أن تحكم على الجاني بإحدى العقوبات التبعية الواردة في المادتين سالفتى البيان إلى جانب الحكم بالعقوبة الأصلية المناسبة للفعل الإجرامي المعاقب عليه وفقاً لأحكام قانون مكافحة جرائم تقنية المعلومات.

وتنقسم هذه العقوبات التبعية المشار إليها في هاتين المادتين إلى ثلاثة أنواع، لكل نوع منها شروط أو حالات يجب توافرها للحكم بها، يمكن أن نجملها فيما يلي:

النوع الأولي: عقوبة المصادرة: للأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها، مع الأخذ في الاعتبار حقوق الغير حسن النية(١).

النوع الثاني: عقوبة الغلق: وتكون في حالة عدم حصول الشخص الاعتباري على ترخيص مزاولة النشاط أو المهنة، فإذا لم يحصل علي هذا الترخيص فيكون على المحكمة أن تقضي إلى جانب العقوبة الأصلية بعقوبة الغلق، ولكن بشرط أن يكون القانون قد تطلب لمزاولة هذا النشاط الحصول على

(١) تنص الفقرة الأولي من المادة ٣٨ من القانون على أنه "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها.

ترخيص من احدي الجهات الحكومية[١].

<u>النوع الثالث: العزل من الوظيفة</u>: وتكون في حالة إذا كان الجاني موظف عام، وكان قد ارتكب الجريمة أثناء مباشرة مهام وظيفته أو بسببها، والعزل نوعان، عزل اختياري وعزل وجوبي[٢]:

١-**يكون العزل اختياري:** في جميع الأحوال طالما تعلقت الجريمة بموظف عام أثناء أو بسب مباشرة أعمال وظيفته.

٢-**يكون العزل وجوبياً:** إذا ما توافرت احدي الحالات الواردة في المادة ٣٤ من ذات القانون، وهي حالة إذا ما وقعت الجريمة بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي.

وقد سلك المشرع الكويتي في المادة الثالثة عشر منه ذات نهج المشرع المصري والتي نصت على أن "يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي أرتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية أو بحق المضرور في التعويض المناسب. ويكون الحكم بإغلاق المحل أو الموقع وجوبيا إذا تكرر

---

(١) تنص الفقرة الثانية من المادة ٣٨ من ذات القانون على أن "وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلا عن العقوبات المقررة بالغلق.

(٢) تنص المادة ٣٩ من القانون على أن "للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضي بعزله مؤقتا من وظيفته مؤقتا، إلا في الحالات المشار إليها في المادة (٣٤) من هذا القانون فيكون العزل وجوبيا.

ارتكاب أيا من هذه الجرائم بعلم مالكها.

وعلى رغم من تشابه هذا الاتجاه المتبع من جانب المشرع الكويتي مع اتجاه المشرع المصري في النص على الأخذ بهذه العقوبات التكميلية أو التبعية، إلا أنهما اختلفا في عدة جوانب تتلخص في الآتي:

أولاً: أوجه التشابه: في تناولهما النص على عقوبتي المصادرة والغلق، إلا أن المشرع الكويتي كان موفقاً في تقييد عقوبة الغلق بمدة محددة وهي مدة سنة واحدة.

ثانياً: أوجه الاختلاف: بالنسبة للمشرع المصري فقد كان موفقاً في النص على عقوبة العزل كعقوبة تبعية أو تكميلية للعقوبة الأصلية في حالة إذا ما كان الجاني موظف عام حكومي، سواء أكان العزل اختياريا يترك لسلطة القاضي أو إجبارياً في حالات معينة على النحو المتقدم، في حين أن المشرع المصري أغفل النص على عقوبة التعويض.

أما المشرع الكويتي، فقد أغفل النص على هذه العقوبة وهي العزل من الوظيفة، إلا أنه كان موفقاً في النص على عقوبة التعويض المناسب الجابر للأضرار المترتبة على هذه الانتهاكات والجرائم التي تقع من الجاني.

وعلى الجانب السعودي، فقد قصر المشرع في المادة الثالثة عشر منه العقوبات التبعية على عقوبتين فقط، هما عقوبة المصادرة وعقوبة الغلق، دون غيرهما[1].

وبالنسبة للمشرع الإماراتي فقد تناول بالنص العديد من العقوبات التبعية،

---

(١) تنص المادة ١٣ من القانون السعودي على أن "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقتًا متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه".

منها ما هو متشابه مع ما جاء في التشريعين السابقين، ومنها ما هو مستحدث، حيث تضمنت المادة ٤١ من القانون[١] النص على عقوبة المصادرة للأجهزة والآلات والوسائل المستخدمة، إضافة للحكم بإغلاق الموقع أو المحل الذي ارتكبت منه الجريمة، سواء أكان إغلاقاً كلياً أو للمدة التي تقدرها المحكمة، وهما عقوبتان تتشابهان مع ما جاء في التشريع المصري والكويتي على النحو سالف البيان.

ومن العقوبات التبعية الجديد والمستحدث التي لم يتنبه لها غيره من أصحاب التشريعات المقارنة، ما جاء في المادتين ٤٢، ٤٣ من ذات القانون وهي[٢]:

١- عقوبة الإبعاد عن البلاد كعقوبة تبعية أو تكميلية تطبق على الأجنبي بعد تنفيذ العقوبة المحكوم بها عليه وتمام نفاذها.
٢- عقوبة وضع المحكوم عليه تحت الإشراف أو المراقبة.
٣- عقوبة حرمان المحكوم عليه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلوماتية أخرى.
٤- عقوبة وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل للمدة التي

---

(١) يراجع نص المادة ٤١ من ذات القانون الإماراتي التي تنص على أنه " مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة.

(٢) تنص المادة ٤٢ من ذات القانون بعد التعديل على أنه " مع مراعاة حكم الفقرة الثانية من المادة (١٢١) من قانون العقوبات تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها". وتنص المادة ٤٣ منه على أن " مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة ".

تراها المحكمة مناسبة .

وبذلك يكون المشرع الإماراتي موفقاً إلى حد كبير في التوسعات التشريعية التي أتى بها في هذا الجانب الإجرائي، وأدعو المشرع المصري أن يحزو حزوه بإضافة عقوبات تبعية أو تكميلية جديدة، ومنها على وجه الخصوص إضافة عقوبة النشر بحيث يتم نشر العقوبات والأحكام التي تصدر في جريدتين يوميتين واسعتي الانتشار على نفقة الجاني سواء أكان شخص طبيعي أو اعتباري حتى تكون رادعاً له ولغيره، إضافة إلى نشر التوعية الجنائية أو العقابية لجميع الطوائف بخطورة هذه الجرائم التقنية، كما أرى ضرورة أن تكون كافة الأحكام التكميلية أو التبعية وجوبيه للقاضي لا اختيارية .

المطلب الثالث

الأحكام العامة المتعلقة بالعقوبة

تمهيد:

تضمن قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية مجموعة من الاجراءات العامة المتعلقة بتطبيق العقوبة وتوابعها، وقد أنقسمت هذه الأحكام وفقاً لنصوص قانون مكافحة جرائم التقنية المعلوماتية إلى أربعة أنواع ضوابط التشديد والإعفاء من العقوبة شاملة الظروف والأسباب الدافعة لإتباع هذا الاتجاه، والأحكام المتعلقة بالصلح أو التصالح، والشروع في الجريمة، وأحكام المسئولية الجنائية، وهو ما سنتناوله تفصيلاً من خلال التقسيم التالي.

تقسيم:

سوف نقول بدراسة هذه الأحكام من خلال تقسيم دراسة هذا المطلب إلى أربع فروع، كما يلي:

الفرع الأول: ضوابط التشديد والإعفاء من العقوبة.

الفرع الثاني: أحكام الصلح والتصالح في الجريمة.

الفرع الثالث: أحكـــام الشـــروع في الجريمـــة.

الفرع الرابع: أحكـــام المسئولية الجنائية.

الفرع الأول

ضوابط التشديد والإعفاء من العقوبة

أولاً: ظروف وأسباب تشديد العقوبة:

لقد حدد المشرع المصري في المادة ٤٣ من الفصل السادس من القانون حالات تشديد العقوبة المقضي بها لتكون السجن المشدد على سبيل الحصر دون تزايد أو توسع فيها، وهذه الحالات هي: حالة إذا ما وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي.

وفي التشريع الإماراتي حدد المشرع الأسباب والظروف الداعية لتشديد العقوبة في الفقرتين الأولي والثانية من المادة ٤٦ من قانون مكافحة تقنية المعلومات، في حالتين هما[١]:

١- إذا ما استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون .

٢- إذا ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة.

---

(١) تنص المادة ٤٦ من القانون الإماراتي على أنه" يعد ظرفاً مشدداً استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون . كما يعد ظرفا مشددا ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة".

وقد تلاحظ لنا أن المشرع الإماراتي أوجب تشديد العقوبة في أضيق حدود بالمقارنة بالمشرع المصري، واسقط أو تجاهل العديد من الحالات الهامة التي تستوجب تشديد العقوبة منها الحالات التي ترتب فيها الجريمة تهديداً لأمن الدولة الاقتصادي، وتعطيل أحكام الدستور والقوانين والإضرار بالوحدة الوطنية وإثارة الذعر والفوضى داخل الدولة وعرقلة ممارسة سلطات الدولة لمهامها واختصاصاتها .

وبالنسبة للمشرع الكويتي فقد جاء في المادة الحادية عشر منه مؤكداً على ضرورة تشديد عقوبة الحبس أو الغرامة المقررة عن نصف حدها الأقصى إذا ما اقترنت الجريمة بإحدى الحالات الآتي[١]:

١- ارتكاب الجريمة من خلال عصابة منظمة .
٢- شغل الجاني وظيفة عامة وارتكابه لها مستغلا سلطته أو نفوذه.
٣- التغرير بالقصر ومن في حكمهم من ناقصي الأهلية أو استغلالهم.
٤- صدور أحكام سابقة من المحاكم الوطنية، أو الأجنبية بموجب الاتفاقيات المصادق عليها بإدانة الجاني بجرائم مماثلة.

وهذا الاتجاه أتفق تماماً وتشابه كلياً مع اتجاه المشرع السعودي في المادة الثامنة من نظام مكافحة جرائم تقنية المعلومات السعودي[٢]، هو تصرف محمود واتجاه حسن من كلا المشرعين الكويتي والسعودي، وكانا موفقين في الصياغة القانونية وملمان بأهم الحالات التي تستوجب التشديد، خاصة ما يتعلق بالتغرير بالقصر أو ناقصي الأهلية واستغلالهم، وهى حالات لم نري لها مثيل في باقي

---

(١) يراجع نص المادة (١١) من التقنين الكويتي سالف البيان.

(٢) تنص المادة المادة الثامنة من التقنين السعودي على أنه " لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية: ١- ارتكاب الجاني الجريمة من خلال عصابة منظمة. ٢- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه. ٣- التغرير بالقُصَّر ومن في حكمهم، واستغلالهم. ٤- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

التشريعات، وإن كنا نتمنى أن يزيدا عليها حالات أخري منها ما أورده المشرع المصري على النحو المتقدم، ومنها حالات لم ترد به مثل إثارة الفوضى والذعر وتهديد الأمن الاقتصادي وغيرها.

ثانياً: أحكام التخفيف والإعفاء من العقوبة:

جاءت المادة ٤١ من القانون المصري متضمنة إعفاء المتهم بارتكاب جريمة ما أو الاشتراك فيها من العقوبة المقررة للجريمة في حالات وظروف معينة، وهي[١]:

١- إذا بادر أياً من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عن الجريمة قبل البدء في تنفيذها وقبل كشفها.
٢- يجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكن الجاني أو الشريك، في أثناء التحقيق، السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة.
٣- إذا أعان السلطات المختصة أثناء البحث والتحقيق على كشف الحقيقة، أو على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة.

وفي جميع الأحوال لا يؤثر هذا الإعفاء على حق الدولة في تحصيل المبالغ التي استحوذ عليها أو تحصل عليها المتهم من خلال احدي الجرائم المرتكبة والمنصوص عليها في هذا القانون، فيجب القضاء برد المبلغ المتحصل عليه حتى

---

(١) تنص المادة ٤١ على أن" يعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها. ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكن الجاني أو الشريك، في أثناء التحقيق، السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة. ولا يخل حكم هذه المادة، بوجوب القضاء برد المال المتحصل من الجرائم المنصوص عليها في هذا القانون".

وإن قضي بالإعفاء من العقوبة أو التخفيف من حدها .

وقد أجاز المشرع الإماراتي للمحكمة التخفيف من حد العقوبة المقررة للجريمة أو الإعفاء منها نهائياً وذلك بناء على طلب من النائب العام، وهذا التخفيف أو الإعفاء مقرر لمصلحة كل من أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم(١).

ويؤخذ على المشرع الإماراتي أنه قيد سلطة الإعفاء وقصرها على جهة واحدة محددة دون غيرها بربطها بضرورة أن تتم بناء على طلب من النائب العام فقط، وهو بذلك حظر على المحكمة أن تقضي به من تلقاء نفسها، وهو اتجاه منتقد وغير موفق وقع فيه المشرع الإماراتي .

وقد تشابه اتجاه المشرع الكويتي في المادة (١٢) مع بعض ما قرره المشرع المصري من ضوابط لتطبيق الإعفاء من العقوبة في جرائم تقنية المعلومات، حيث نص هذه المادة على أن " للمحكمة أن تعفي من العقوبة كل من بادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة، فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق تعين للإعفاء من العقوبة أن يكون من شأن الإبلاغ ضبط باقي الجناة في حالة تعددهم".

وهو ذات ما تبناه المشرع السعودي أيضاً في المادة الحادية عشر من نظام المكافحة التقنية السعودي والتي جاء بها أن " للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون

---

(١) تنص المادة ٤٥ من القانون الإماراتي على أن" تقضي المحكمة، بناء على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم ".

من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة" .

الفرع الثاني

أحكام الصلح والتصالح في الجريمة

المشرع المصري كان سباقاً عن غيره بالنص على جواز إمكانية الصلح أو التصالح في مثل هذه الجرائم، وهو اتجاه لم يتبناه غيره من مشرعي الدول المقارنة، خاصة وأن المشرع المصري تناول هذا التنظيم الإجرائي بكل دقة وبراعة فنية وإجرائية من حيث صياغة ضوابط إجراء عملية الصلح والتصالح في الجريمة المعلوماتية على الرغم من وجود بعض المأخذ التي سوف نوردها فيما بعد.

فقد أورد المشرع في الفقرة الأول من المادة (٤٢) من القانون المصري[١] جواز إمكانية التصالح فيما بين المتهم والمجني عليه أو وكيله الخاص أو خلفه العام، في أي مرحلة كانت عليها الدعوي، وقبل أن يصبح الحكم فيها باتاً، واثبات ذلك أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، ولكنه لم يبيح هذا التصالح في كافة الجرائم المعلوماتية المرتكبة، ولكنه قيده بنوع معين من الجرائم وهي جرائم الجنح الواردة في نصوص محددة بالقانون، وهذه النصوص هي (١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) .

ويبقي هنا التساؤل، متى ينتج هذا التصالح أثره، ويتم الاعتراف به وإقراره ؟

---

(١) تنص المادة ٤٢ على أن" يجوز للمتهم في أي حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا، إثبات الصلح مع المجني عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد (١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون. ولا ينتج إقرار المجني عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون. كما لا يقبل التصالح إلا من خلال الجهاز في الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون".

وللإجابة على هذا التساؤل الهام فقد فرق المشرع المصري في الفقرة الثانية من المادة ٤٢ من ذات القانون، بين حالتين، وهما:

الحالة الأولي: تتعلق بالجنح المنصوص عليها في المواد (١٤، ١٧، ١٨، ٢٣) من القانون، وفي هذه الحالة نص المشرع على أن لا يقبل هذا التصالح ولا ينتج أثره إلا باعتماده من قبل الجهاز، ونظمت اللائحة التنفيذية للقانون إجراءات قبول واعتماد صلح المجني عليه في هذه الحالة من قبل الجهاز المختص، حيث اشترطت المادة ١٢ من اللائحة التنفيذية لقبول الصلح واعتماده ضرورة استيفاء تقديم ما يلي[١]:

١- شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة محل الصلح.
٢- صورة طبق الأصل من المحضر أو الوثيقة التي اثبت فيها الصلح بين المتهم والمجني أو وكيله الخاص أو خلفه العام أمام النيابة أو المحكمة المختصة والمتضمنة إقرار المجني عليه بهذا الصلح.
٣- شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي في الدعوي الجنائية.
٤- طلب بأسم الرئيس التنفيذي للجهاز لاعتماد المحضر أو الوثيقة المتضمنة إقرار المجني عليه بالصلح يقدم من المتهم أو من وكيله أو من خلفه العام.

الحالة الثانية: وهي الحالة المتعلقة بالجنح المنصوص عليها في المادتين (٢٩، ٣٥) من هذا القانون، وفيها لا يقبل التصالح إلا من خلال الجهاز ذاته[٢]، وذلك باستيفاء تقديم ما يلي[٣]:

١- شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد

---

(١) يراجع نص المادة ١٢ من اللائحة التنفيذية للقانون سالفة البيان.
(٢) تنص الفقرة ٢ من المادة ٤٢ من القانون على أن" .... كما لا يقبل التصالح إلا من خلال الجهاز في الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون".
(٣) يراجع نص المادة ١٣ من اللائحة التنفيذية للقانون سالفة البيان.

والوصف للجريمة موضوع التصالح.

٢- شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي في موضوع الجريمة محل طلب التصالح.

٣- أن يقدم المتهم الراغب في التصالح أو وكيله قبل رفع الدعوي الجنائية الإيصال الدال على سداده مبلغاً يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة.

٤- أن يقدم المتهم الراغب في التصالح أو وكيله بعد رفع الدعوي الجنائية الإيصال الدال على سداده ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى للغرامة أيهما أكثر قبل صدور حكم نهائي في الموضوع.

وأخيراً نعيب على المشرع المصري في الفقرة الثانية من المادة (٤٢) من القانون إغفاله للعديد من الجرائم الهامة والخطيرة التي سبق وأن أجاز فيها التصالح، فقد تناول في الحالتين عدد من المواد التي يجوز فيها التصالح سوء أن يتم ذلك باعتماد الجهاز، أو من خلاله، وأغفل الجرائم الواردة في المواد (١٥، ١٦، ١٩، ٢٦، ٣٠، ٣١)، إلى جانب النقد الموجه لما شاب نصوص اللائحة التنفيذية في المادتين ١٢، ١٣ من عيوب في الصياغة وعدم الدقة.

ولنا هنا أن نتساءل هل المشرع كان يقصد من وراء هذا الإغفال أن هذه الجرائم يتم فيها التصالح بدون اعتماد من الجهاز المختص ودون علمه؟! فإن كانت الإجابة بنعم فما هي الحكمة من تقييد التصالح في باقي المواد برضاء الجهاز وموافقته، وإن كانت الإجابة بالنفي فلماذا لم يأتي المشرع بتنظيمها ووضع ضوابط لها مثلما فعل مع باقي الجرائم الأخرى.

ونحن من جانبنا لم نجد إجابة على هذا التساؤل الهام، ولم يتفتق ذهننا إلى السبب أو المقصد من ذلك، بل وما هي الحكمة التي قصدها المشرع من هذه التفرقة في النصوص.

ويقول المشرع في الفقرة قبل الأخيرة من ذات المادة أنه وفي جميع الأحوال، يجب على المتهم الذي يرغب في التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغا يعادل ضعف الحد الأقصى للغرامة المقرر للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة، بحسب الأحوال[1].

هذا النص يتناقض إلى حد كبير مع ما جاء بالفقرة الأولي من ذات المادة، كما أنه كيف يصل علم الجاني بالدعوي الجنائية، ففي أغلب الحالات الجاني لا يعلم بالدعوي الجنائية إلا بموجب إعلانه، ولا علم للجاني بنية المجني عليه المتجهة لإقامة الدعوي الجنائية، فكيف يطلب منه إيداع مبلغ مالي يزيد عن قيمة الغرامة المقررة للجريمة ليثبت حسن نواياه واتجاه نيته نحو طلب التصالح، من وجهة نظري أن المشرع هنا لم يحالفه التوفيق في الصياغة وأصابها عدم المعقولية والتناقض .

الفرع الثالث

أحكـام الشـروع في الجريمـة

يقصد بالشروع في الجريمة وفقاً لنص المادة ٤٥ من قانون العقوبات المصري هــو البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها، ولا يعتبر شروعاً في الجناية أو الجنحة مجرد العزم على ارتكابها ولا الأعمال التحضيرية لذلك. وقد عرفه فقه القانون بأنه السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة كادت أن

---

(١) تنص الفقرة الأخيرة من المادة ٤٢ على أن" ولا يسقط حق المتهم في التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائي في الموضوع، وفي جميع الأحوال، يجب على المتهم الذي يرغب في التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغا يعادل ضعف الحد الأقصى للغرامة المقرر للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة، بحسب الأحوال. ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية".

تقع بالفعل لولا تدخل عامل أخر خارج عن إرادة الفاعل حال في اللحظة الأخيرة دون وقوع الجريمة[١] .

فالشارع في الجريمة إذن هو مجرم لم يحالفه الحظ في تمام جريمته لسبب خارج عن إرادته بفعل عامل خارجي غير متوقع الحدوث لا يد له فيه، ولا يعد من قبيل الشروع الأعمال التحضيرية أو مجرد العزم على ارتكاب الجريمة.

وقد عاقب المشرع المصري على فعل الشروع في الجنايات دون حاجة إلى وجود نص خاص ينظمه حيث نص في المادة ٤٦ من قانون العقوبات على أنه "يعاقب على الشروع في الجناية بالعقوبات التالية إلا إذا نص القانون على خلاف ذلك ...."

أما بالنسبة للجنح فالوضع مختلف تماماً إذ أن الأصل لا عقاب على الشروع في الجنحة إلا إذا وجد نص عقابي يجرمه في القانون المجرم لتلك الجنحة، عندئذ يحدد ذلك النص العقوبة المقررة للشروع، وفي ذلك تنص المادة ٤٧ من قانون العقوبات على أنه " تعين قانوناً الجنح التي يعاقب على الشروع فيها وكذلك عقوبة هذا الشروع ".

وقد تبني المشرع في قانون جرائم التقنية المعلوماتية معيار العقاب علي الشروع في الجنح في المادة ٤٠ منه بنصها على أن يعاقب الفاعل حتى على مجرد الشروع في ارتكاب الجريمة، دون تطلب تمام نفاذها وتحقق كافة عناصرها، بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة [٢].

وهذا الإتجاه تبنته أغلب التشريعات المقارنة، حيث تناولها المشرع السعودي في المادة العاشرة التي جاء نصها بأن "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة

---

(١) د. رمسيس بهنام – النظرية العامة للقانون الجنائي، منشأة المعارف، ١٩٩٥، ص٥٨٣.

(٢) تنص المادة ٤٠ من قانون التقنية على أن " يعاقب كل من شرع في ارتكاب الجنح المنصوص عليها في هذا القانون بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة ".

المقررة". وكذا المشرع الإماراتي في المادة ٤٠ التي نصت على أن " يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة".

أما بالنسبة للمشرع الكويتي فقد أغفل النص على معاقبة الجاني في حالة الشروع في ارتكاب الجريمة وعدم تمام حدوثها أو تحقق عناصرها واركنها، وهو اتجاه منتقد ومعيب يؤخذ عليه، وندعوه لأن يعيد النظر في هذا الشأن والتأكيد على إضافة نص خاص يتعلق بفعل الشروع المجرم والعقوبة المقررة عليه أسوة بما فعله اغلب مشرعي القانون المقارن .

الفرع الرابع

أحكـام المسئوليـة الجنائيـة

لم تقتصر اهتمامات المشرع المصري على ما سلف بيانه فقط، بل لقد عني بالعديد من الاهتمامات الأخرى الواضحة والملموسة كان من بينها حرصه على تنظيم أحكام المسئولية الجنائية الناشئة عن جرائم تقنية المعلومات، سواء تعلقت بمقدم الخدمة أو بالمستفيد منها أو بالشخص الاعتباري، حيث تناول في المواد ٣٠، ٣١، ٣٢، ٣٣، ٣٥، ٣٦، ٣٧ ضوابط تنظيم المسئولية الجنائية لكل من مقدم الخدمة، والشخص الاعتباري، وهو ما سوف نتناوله في هذا الجزء من الدراسة، ولكن قبل التطرق لذلك من المتعين علينا أن نستعرض أهم الالتزامات والواجبات الملقاة على عاتق مقدم الخدمة والتي يترتب على إخلالها انعقاد المسئولية الجنائية لأيهما، وذلك على النحو التالي:

أولاً: التزامات وواجبات مقدم الخدمة:

يقصد بمقدم الخدمة وفقاً لأحكام قانون تقنية المعلومات المصري، هو أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن

ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات[1]، ونظراً لأهمية الدور الذي يلعبه مقدم الخدمة فقد أسند إليه المشرع المصري مجموعة من الالتزامات والواجبات العامة وألزمه بضرورة إتباعها ومراعاة تنفيذها.

وقد أورد المشرع النص علي هذه الالتزامات والواجبات المشار إليها في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ سنة ٢٠١٨، وكذا المادة الثانية من اللائحة التنفيذية للقانون رقم ١٦٩٩ لسنة ٢٠٢٠ وقام المشرع بتقسيمها إلى أربعة فئات أو طوائف وذلك على النحو التالي:

الطائفة الأولي: حفظ وتخزين البيانات والمعلومات وضمان سريتها[2]:

أولاً: التزام مقدم الخدمة بحفظ وتخزين سجل النظام المعلوماتى أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة .

ثانياً: المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل

---

(١) يراجع: المادة الأولي من الباب الأول من القانون، المتعلقة بالمصطلحات والمعاني.

(٢) ينص البند (أولاً) من المادة الثانية من قانون التقنية المصري على أن " مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣، يلتزم مقدمو الخدمة بما يأتي:

١- حفظ وتخزين سجل النظام المعلوماتى أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي: (أ) البيانات التي تمكن من التعرف على مستخدم الخدمة. (ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة. (ج) البيانات المتعلقة بحركة الاتصال. (د) البيانات المتعلقة بالأجهزة الطرفية للاتصال. (هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

٢- المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

٣- تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

ذلك البيانات الشخصية لأي من مستخدمي خدمته[١]، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون[٢]، أو الأشخاص والجهات التي يتواصلون معها.

ثالثاً: تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها[٣] أو تلفها.

الطائفة الثانية: واجبات مقدم الخدمة تجاه المستخدم أو أية جهة حكومية مختصة:

ألزم المشرع مقدم الخدمة بضرورة أن يعمل دوماً على توفير البيانات والمعلومات التي تطلب منه من المستخدم[٤] أو أية جهة حكومية مختصة، مع مراعاة أن يتم ذلك بالشكل والطريقة التي يمكن الوصول إليها بطريقة مباشرة وسريعة وميسرة ومستمرة، وقد حدد المشرع هذه البيانات والمعلومات في البند ثانياً من المادة الثانية[٥].

---

(١) البيانات الشخصية: هي أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى. يراجع: المادة الأولي من القانون.

(٢) الحساب الخاص: هو مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.

(٣) الاختراق: هو الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها. يراجع: المادة الأولي من القانون.

(٤) المستخدم هو كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنية المعلومات، أو يستفيد منها بأي صورة كانت. يراجع في ذلك: المادة الأولي من القانون.

(٥) ينص البند (ثانياً) من المادة الثانية من قانون التقنية المصري على أن " مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية: "١- اسم مقدم الخدمة وعنوانه. ٢- معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني. ٣- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي

الطائفة الثالثة: تتعلق بتقديم الدعم الفني وتوفير الإمكانيات اللازمة لجهات الأمن القومي[١]:

حيث ينص البند (ثالثاً) من المادة الثانية على أن " مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقا لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون".

الطائفة الرابعة: تتعلق بضرورة أن يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك[٢].

وهذا التنظيم الذي أتى به المشرع المصري، لم نجد له مثيل في تشريعات الدول الأخرى المقارنة، ولذلك كان المشرع المصري أكثر اهتماماً وحرصاً من غيره في كافة جوانب هذا القانون، وأحاط عملية المكافحة من جميع النواحي والجهات المتعلق بها.

ثانياً: المسئولية الجنائية لمقدمي الخدمة:

حرص المشرع الأوروبي على تنظيم مسئولية مقدمي الخدمة، فقد تبني التوجيه الأوربي الصادر بشأن التجارة الالكترونية في ٨ يونيو ٢٠٠٠[٣] نظاماً

يخضع لإشرافها. ٤- أي معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المختص.".

(١) الأمن القومي: هو كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي، ووزارة الدفاع والإنتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات.
وجهات الأمن القومي: هي رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

(٢) يراجع البند (رابعاً) من المادة الثانية سالفة البيان.

(٣) صدر التوجيه الأوروبي في ٨ يونيو ٢٠٠٠ بهدف تحقيق التجانس بين تشريعات الدول الأوروبية بشأن نظام مسئولية مقدمي الخدمات عبر الانترنت، وتأكيد ضرورة التوازن بين مصلحة مقدمي

مرناً بشأن مسئولية مقدمي خدمات الانترنت بوجه عام، فحظر في المادة ١٥/ ١ منه على الدول الأعضاء فرض التزام عام على هؤلاء، سواء برقابة المعلومات التي يتم تداولها أو تخزينها، أو البحث عن الوقائع أو الملابسات التي تشير إلى وجود نشاط غير مشروع[١]، ومع هذا فقد أجازت المادة ١٥/ ٢ من ذات التوجيه على فرض نوع من الرقابة المحدودة والمؤقتة على هذه المواقع في بعض الأحوال[٢] .

وقد سار على هديه المشرع الفرنسي فقد حرص على معالجة مسئولية مقدمي الخدمة أكثر من مرة كان أولها بإصداره قانون أول أغسطس ٢٠٠٠، ثم ألحقه بإصدار قانون LCEN[٣] رقم (L. n° 2004-575) في ٢١ يونيو ٢٠٠٤ الذي حل محل القانون السابق متأثراً بما ورد بالتوجيه الأوروبي سالف الذكر من نصوص، حيث لم يضع صراحة أية نصوص تشير إلى مسئولية متعهد الخدمة أو الوصول، وإنما اكتفي بالنص في المادة ٦/ ٨ على أن للقضاء أن يصدر أمراً على عريضة في مواجهة متعهد الوصول أو الإيواء، بإلزام أي منهما باتخاذ التدابير اللازمة لتفادي وقوع الضرر أو وقفه حال حدوثه.

ومؤدي ذلك أن مسئولية متعهد الوصول لا تقوم إلا إذا صدر – مسبقاً – أمر على عريضة بإلزامه بوقف بث المضمون الالكتروني غير المشروع واتخاذ

الخدمات، من جهة، وحماية أصحاب الحقوق في مواجهة القرصنة الالكترونية من جهة أخري، حيث وضع مبدأ عاماً مفاده عدم مسئولية مقدمي الخدمات الالكترونية إلا في أحوال معينة، وبشروط خاصة، وسمي ذلك بالمسئولية المشروطة أو عدم المسئولية (non-responsabilité ou conditionnelle). يراجع في ذلك أحكام المواد ١٤، ١٥ من التوجيه الأوروبي: ويراجع أيضاً:

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 sur le commerce éléctronique, JOCE, n° L.178 du 17 juillet 2000, p.1.

(1) G. Haas et O. de Tissot, L'activité du fournisseur d'hébergement à l'epreuve des droits des tiers: Com. Comm. Électr. Juillet-août 2000, chron. P. 16.

(٢) د/ اشرف جابر سيد– مسئولية مقدمي خدمات الانترنت عن المضمون الالكتروني غير المشروع (دراسة خاصة لمسئولية متعهدي الإيواء)، مجلة كلية الحقوق جامعة حلوان للدراسات القانونية والاقتصادية، العدد الثاني والعشرون، يناير– يوليو ٢٠١٠، ص٢١.

(٣) اختصارا لعبارة (Loi sur La Confiance dans L'Economie Numérique).

التدابير اللازمة لذلك، وعدم تقيده بهذا الأمر، أو بمعني أدق أن المادة ٦ سالفة البيان فرضت على مقدم الخدمة أو متعهد الوصول التزاماً مقتضاه تبصير عملائه بوسائل التقنية التي تسمح بتقييد الوصول إلى بعض الخدمات، أو إرشادهم إليها، أو إلى أكثرها فعاليه، واعتبرت إخلاله بهذا الالتزام إهمال من جانبه[١]، ولكنها من ناحية أخري لم تقرر جزاء جنائياً عن الإخلال بهذا الالتزام، ولو بفرض غرامة على متعهد الوصول[٢].

وتأكيداً لهذا الاتجاه التشريعي نصت المادة التاسعة من ذات القانون على أن متعهد الوصول لا يسأل كمبدأ عام إلا إذا كان هو مصدر تداول المعلومات أو قام بوضع أو تعديل المضمون محل التداول[٣].

أما بالنسبة لموقف المشرع المصري في هذا الشأن فقد كان أكثر صراحة من غيره في تنظيم قواعد مسئولية مقدم الخدمة، حيث تناول في المواد من ٣٠ : ٣٣ من قانون مكافحة جرائم تقنية المعلومات معاقبة مقدم الخدمة إذا ما أهمل، أو أخل بأحد الالتزامات والواجبات الملقاة على عاتقه والملزم بمراعاتها، وأوقع عليه مسئولية جنائية حال إخلاله وتقاعسه بذلك، وقسم المشرع ضوابط هذه المسئولية إلى أربعة حالات، وذلك على النحو التالي:

الحالة الأولي[٤]: إذا امتنع مقدم الخدمة عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في

---

(1) J. Passa, Propriété littéraire et artistique, internet et droit d'auteur, JCP Civil annexes, fasc. 1970.& Morgan Lavanchy, La responsabilité délictuelle sur Internet en droit Suisse, mém. 2002, p.44.

(2) Rapport de J. Cédras (avocat général à la Cour de Cassation) remis au Ministre de la Culture et de la Communication, Le téléchargement illicit d'oeuvres protégées par le droit d'auteur, avril 2007, cite par Simon Warynski, précité, p. 8 .

(3) L'Article 9 : le fournisseur daces nest pas en Principe responsable du contenu sauf s'il est « à l'origine de la transmission litigieuse» ou s'il « sélectionne ou modifie les contenus faisant l'objet de la transmission» .

(٤) ورد النص على هذه الحالة في المادة (٣٠) من قانون مكافحة جرائم تقنية المعلومات المصري.

الفقرة الأولى من المادة (٧) من هذا القانون، وفي هذه الحالة يعاقب الممتنع بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين.

أما إذا ترتب على هذا الامتناع أضرار تمثلت في وفاة شخص أو أكثر، أو الإضرار بالأمن القومي، ففي هذه الحالة تشدد المشرع وضاعف من العقوبة المقررة وجعلها السجن المشدد، والغرامة التي لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضي المحكمة فضلا عن ذلك بإلغاء ترخيص مزاولة النشاط.

الحالة الثانية[١]**:** إذا خالف مقدم الخدمة الأحكام الواردة بالبند (٢) من الفقرة أولاً من المادة الثانية من القانون، والمتعلقة بالمحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

وجعل المشرع العقوبة المقررة في هذه الحالة هي الحبس مدة لا تقل سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة.

الحالة الثالثة[٢]**:** إذا امتنع مقدم الخدمة عن تنفيذ القرار الصادر إليه من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها في المادة (٦) من هذا القانون، والتي تتعلق بنظام معلوماتي أو جهاز تقنى موجود تحت يديه وسيطرته، أو مُخزن لديه، أو بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني .

---

(١) ورد النص على هذه الحالة في المادة (٣١) من ذات القانون.

(٢) ورد النص على هذه الحالة في المادة (٣٢) من ذات القانون.

وفي هذه الحالة يعاقب الممتنع بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

الحالة الرابعة[1]: تتعلق بمعاقبة مقدم الخدمة الذي يخالف الالتزامات والواجبات المفروضة عليه في المادة الثانية من القانون، وذلك على النحو التالي:

١- يعاقب بغرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه، كل مقدم خدمة أخل بأي من التزاماته المنصوص عليها في البند (١) من الفقرة (أولاً) من المادة (٢) من هذا القانون. وتضاعف عقوبة الغرامة في حالة العود، وللمحكمة أن تقضي بإلغاء الترخيص.

٢- ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثانيا) و(رابعاً) من المادة (٢) من هذا القانون.

٣- ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثالثاً) من المادة (٢) من هذا القانون.

وبتدقيق النظر في تشريعات الدول المقارنة بحثاً عن تنظيم تشريعي للمسئولية الجنائية لمقدم الخدمة الناشئة عن جرائم تقنية المعلومات أسوة بالمشرع المصري فلم نجد لها مثيل وأصابها جميعاً القصور والإغفال الصريح، ويتبين أن المشرع المصري كان متفرداً وبارزاً في تناول هذا التنظيم التشريعي، وهو اتجاه موفق من جانبه.

ثالثاً: المسئولية الجنائية للشخص الاعتباري:

كما أهتم المشرع المصري وكان حريصاً أيضاً على تنظيم أحكام المسئولية الجنائية المتعلقة بالشخص المعنوي وأفرد لها نصوصاً خاصة بها في المواد من ٣٥: ٣٧ من القانون، حيث جعل المسئولية الجنائية لهذا الشخص المعنوي تنعقد

(١) يراجع نص المادة (٣٣) من القانون المصري الصادر بشأن مكافحة جرائم تقنية المعلومات.

إذا ما توافرت أحدي الحالات الآتي:

الحالة الأولي[1]: إذا ما تعرض الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتى المخصص لكيان معنوي، لأي جريمة من الجرائم المنصوص عليها في هذا القانون، ولم يقم الشخص المسئول عن الإدارة الفعلية لهذا الكيان، أو الشخص المعنوي، بتبليغ الجهات الرسمية المختصة وقت علمه بالجريمة، وفي هذه الحالة يعاقب المسئول عن إدارة هذا الكيان بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تزيد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين، نظير تقاعسه وإهماله.

الحالة الثانية[2]: والتي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون بأسم ولحساب الشخص الاعتباري، في هذه الحالة تنوعت العقوبة المقضي بحيث يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي.

كما أنه للمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها أيضاً في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري.

وفي جميع الأحوال، ليس معني انعقاد المسئولية الجنائية للشخص المسئول عن الإدارة الفعلية للشخص الاعتباري استبعادها أو انتفائها بالنسبة للشخص الطبيعي مرتكب الجريمة، فقد حرصت المادة (٣٧) من القانون على التأكيد على انعقاد المسئولية الجنائية للأشخاص الطبيعيين سواء أكانوا فاعلين أصليين أو شركاء عن ذات الوقائع التي تقوم بها الجريمة إلى جانب مسئولية المسئول عن

---

(١) يراجع نص المادة (٣٥) من ذات القانون المصري.

(٢) يراجع نص المادة (٣٦) من القانون المصري.

إدارة الكيان أو الشخص المعنوي[1].

وقد توافق هذا الاتجاه مع مسلك المشرع الكويتي المتبع في المادة الرابعة عشر من قانون مكافحة جرائم التقنية، التي نصت على أنه " مع عدم الإخلال بالمسئولية الجزائية الشخصية لمرتكب الجريمة، يعاقب الممثل القانوني للشخص الاعتباري بذات العقوبات المالية المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا ثبت أن إخلاله بواجبات وظيفته أسهم في وقوع الجريمة مع علمه بذلك .

ويكون الشخص الاعتباري مسئولا عما يحكم به من عقوبات مالية أو تعويضات إذا ارتكبت الجريمة لحسابه أو بأسمه أو لصالحه" .

(١) تنص المادة (٣٧) من ذات القانون على أنه" في تطبيق أحكام هذا القانون، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتباري استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التي تقوم بها الجريمة".

الخاتمـــة

لقد ساعد ازدهار الحضارة، وانتشار التقدم التقني في تسهيل الكثير والكثير من أمور الإنسان الحياتية، وأدي إلى السهولة واليسر في تبادل المعلومات والبيانات بواسطة الانترنت ووسائل التقنية الحديثة، ولكنه في نفس الوقت خلف العديد من المخاطر والأضرار المتعلقة بتقنية المعلومات لا سيما وضعف الرقابة عليها، مما أدي إلى ظهور نوع جديد من الجرائم المختلفة تماماً عن الجرائم التقليدية من حيث طريقة وأسلوب ارتكابها، وشكل وصفات المجرم وطباعة سُميت بجرائم التقنية المعلوماتية، وأصبحت تُمثل تهديداً مباشراً وواضحاً للأمن والاستقرار المحلي والعالمي، وعائقاً يحول دون إتمام عملية التطوير والتنمية، ولم تقتصر عواقبه وآثاره على المستوي الفردي والجماعي فقط، بل امتدت لتهدد المجتمع الدولي بأكمله، خاصة وأن هذه الطائفة من الجرائم تتميز بأنها معقدة للغاية لتنوعها، وسهولة ارتكابها، وقدرة الجناة على التخفي والهرب، مما يصعب معه اكتشافها، واثبات أدلتها، وضبط مرتكبها، وإسنادها إليهم.

وتعد هذه الدراسة وسيلة للتعرف على السياسة التشريعية الحديثة التي اتبعها كل من المشرع المصري ومشرعي بعض الدول المقارنة لمواجهة هذا الشبح الخفي، ومكافحة الجريمة التي ترتكب بواسطة وسائل التقنية الحديثة أو من خلالها، ومدي نجاح هذه الجهود التشريعية في المواجهة والتصدي لها، والتعرف على العقوبات التي تضمنتها ومدي كفايتها من خلال ثلاثة محاور رئيسية، المحور الأول انصب على دراسة الأحكام العامة لقانون تقنية المعلومات، من خلال التعرف على ماهية جرائم تقنية المعلومات، وبيان الجهود التشريعية المبذول في مكافحة الجريمة التقنية على المستويين العربي والأوروبي، ثم التعرف على ضوابط تطبيق القانون في مجال التعاون الدولي والنطاق المكاني والاختصاص القضائي للقانون.

والمحور الثاني خصص للتعرف على أهم أنماط أو أنواع الجرائم التقنية، وحدود العقوبات المقررة عليها، أما المحور الثالث فقد تناول مجموعة الأحكام

الإجرائية الخاصة بمكافحة الجرائم التقنية، من حيث إجراءات جمع الاستدلالات من ضبط وتفتيش، وإجراءات الاستعانة بالخبرة الفنية، وبيان مدي حجية الأدلة الرقمية، ثم تعرفنا على التدابير أو الإجراءات التحفظية، والعقوبات التبعية أو التكميلية، وأخيراً الأحكام العامة المتعلقة بالعقوبة، وضوابط التشديد والإعفاء منها، وبيان الأحكام الخاصة بالصلح والتصالح في الجريمة، والشروع فيها، وضوابط وأحكام المسئولية الجنائية الناشئة عنها.

نتائج البحث:

من خلال هذه الدراسة رأينا كيف تصدت العديد من دول العالم لهذا الخطر التقني، وحرصت على تطوير نظم المكافحة التشريعية لديها، بإدخال نصوص تشريعية تتوافق مع ظاهرة الإجرام التقني الحديثة، خاصة على الجانب التشريعي العربي، لتكفل لها الحماية اللازمة من مثل هذه الاعتداءات والمخاطر، ونشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها وبيان وسائل وطرق الوقاية منها.

ورأينا أيضاً كيف كان المشرع المصري متطوراً وموفقاً إلى حد كبير في إصدار العديد من التشريعات والنصوص، ووضع الحلول التشريعية اللازمة، أو المناسبة لمكافحة هذه الجرائم الناشئة عن استخدام وسائل التقنية المعلوماتية، أو الحد منها بالمقارنة بغيره من أصحاب التشريعات المقارنة، وسلامة صياغتها، وخروجه عن نطاق المكافحة التقليدية التي أصبحت لا تتناسب وهذا الإجرام التقني الحديث، نظراً لما تتميز به جرائم تقنية المعلومات من السهولة في ارتكابها، والقدرة على إخفاء أدلتها وآثارها، وقدرة الجناة على الهرب، وشعورهم بأنهم خارج حدود الرقابة والسيطرة القانونية والأمنية .

وتعرفنا من خلال هذا البحث على أهم المصطلحات العلمية والقانونية التى تضمنها القانون المصري رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية، وأهم الجرائم التقنية وحدود العقوبات المقررة لها، كما تعرفنا على أهم الاحكام الاجرائية

المنظمة لمكافحة هذه الظاهرة الاجرامية التقنية، وكيفية التصالح فيها، وضوابط التعاون الدولي في مكافحتها والحد منها .

التوصيات:

توصلنا من خلال هذه الدراسة إلي مجموعة من التوصيات كان من أهمها:

١- دعوة المشرع المصري إلى إعادة النظر في قانون مكافحة جرائم تقنية المعلومات والنص صراحة على بعض الجرائم التقليدية التي تطورت وأصبحت ترتكب بواسطة وسائل التقنية الحديثة مثل (النصب، والتزوير، والقرصنة، والسرقة، وانتحال الصفة، والتحرش والإرهاب الالكتروني، وانتهاك الخصوصية والإساءة للغير، والتجسس...الخ) وإدراجها في نصوص عقابية رادعة تتناسب وخطورتها .

٢- ضرورة وضع نصوص إجرائية تنظيمية تتعلق بإجراءات تحريك الدعوي القضائية ومباشرة الخصومة أمام الجهات القضائية والطعن في الأحكام.

٣- دعوة المشرع المصري لضرورة إعادة النظر في تحديد القاضي الجنائي المختص بنظر الجرائم والنزاعات الناشئة عن استخدام وسائل التقنية المعلوماتية أسوة بجرائم قانون تنظيم الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣، حيث أن قانون المحكمة الاقتصادية رقم ١٢٠ لسنة ٢٠٠٨ لم يتضمن صراحة إسناد الولاية القضائية للمحكمة الاقتصادية بنظر هذا النوع من الجرائم التقنية وقصرها في المادة الرابعة منه على الآتي " تختص الدوائر الابتدائية والاستئنافية بالمحاكم الاقتصادية، دون غيرها، نوعيا ومكانيا بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها في القوانين الآتية: .....١٦- قانون تنظيم الاتصالات.١٧- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات".

٤- دعوة مشرعي الدول المقارنة للتوسع في إدراج نصوص عقابية تتناسب وخطورة بعض الجرائم المعلوماتية أسوة بالمشرع المصري.

٥- دعوة مشرعي الدول المقارنة إعادة النظر في نصوصها التشريعية والعقابية

مع الأخذ في الاعتبار تلافي الانتقادات والمأخذ التي تم توجيهها لهذه التشريعات كل في نطاقه.

٦- دعوة مشرعي الدول المقارنة إلى تضمين نصوصها التزامات وواجبات مقدمي خدمات تقنية المعلومات والمسئولية الواقعة عليهم حال الإخلال بذلك أسوة بالمشرع المصري.

٧- عقد دورات تدريبية مكثفة في مراكز فنية متخصصة لتدريب رجال ومأموري الضبط القضائي وإعداد وتنمية الكوادر الفنية المتخصصة للاستعانة بهم في معاونة رجال الأمن والقضاء في كشف الجريمة والتحقيق فيها.

٨- عقد دورات تدريبية لأعضاء النيابة العامة والقضاة لتثقيفهم فنياً والإلمام بالأمور الفنية التي تعينهم على كشف الجرائم المعلوماتية التقنية والتحقيق فيها ومعرفة عناصرها وأسرارها.

٩- الدعوة للاهتمام بدور الخبرة الفنية المتخصصة في مجال تقنية المعلومات وتفعيل الاستعانة بخبراء التقنية وجعل التقارير الفنية الصادرة عنهم إلزامية أي الخروج بها من مرحلة الاستشارية إلى الإلزامية لأهميتها في كشف ملابسات وطلاسم الجريمة.

١٠- الدعوة إلى عقد المزيد من المؤتمرات والندوات التثقيفية والتوعية بأهمية وخطورة وسائل التقنية المعلوماتية، والتعريف بالعقوبات التي تنتظر من يتجاوز حدود الاستخدام المشروع لهذه الوسائل أو تسخيرها للإضرار بالغير بالمخالفة للقانون.

١١- دعوة المجتمع الدولي العربي لإبرام المزيد من الاتفاقيات والمعاهدات المتعلقة بهذا الشأن لتوحيد الجهود التشريعية في مجال المواجهة الدولية لهذا الخطر التقني والتعاون الفعال في تطبيق قواعد تسليم المجرمين الهاربين مع الأخذ في الاعتبار الاتفاقيات والمعاهدات الدولية الأوروبية.

١٢- دعوة الجامعات المصرية والعربية لإنشاء قسم خاص بجميع الكليات

سواء أكانت كليات الحقوق أم غيرها من الكليات الأخرى لدراسة كل ما هو جديد في مجال تقنية المعلومات وجرائم الانترنت وقانون مكافحة جرائم تقنية المعلومات للتوعية والتثقيف القانوني والتعرف على خطورتها.

١٣- حث الجامعات والمراكز العلمية البحثية على ضرورة تشجيع البحث والدراسة في هذا المجال التقني وتوفير سبل الدعم والمساعدة للباحثين والمتخصصين والعمل على إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم التقنية المعلوماتية وجرائم الانترنت وتكنولوجيا المعلومات.

١٤- ضرورة إصدار كتيب أو دليل إرشادي قانوني يتضمن صور الجرائم التقنية والنصوص العقابية المقررة عليها، والأصول العلمية واجبة الإتباع لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية التقنية، وكافة القرارات والتعليمات التنظيمية الصادرة في هذا الشأن، على أن يراعي تحديثها بشكل دوري كلما دعت الحاجة لذلك ووفقاً للتطورات التي قد تحدث، تحت إشراف وزارة العدل وبالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات، والعمل على تعميم ذلك الدليل على العاملين والمتخصصين والباحثين في الشأن القانوني وأجهزة الشرطة وأعضاء النيابة والقضاة.

١٥- بث موقع الكتروني خاص يكون مفتوحاً للجميع للرد على كافة الشكاوي والاستفسارات المتعلقة بتطبيق أحكام قانون مكافحة تقنية المعلومات ولائحته التنفيذية ونشر كل ما هو جديد في مجال التقنية وتكنولوجيا المعلومات من الناحية الفنية والقانونية .

قائمة المراجـــع

أولا: المراجـــع العربية:

الكتب العلميـــة:

١- **د/ أحمد شوقي عمر أبو خطوة**- شرح الأحكام العامة لقانون العقوبات، الجزء الأول – النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ١٩٩٩.

٢- **د/ أسامة عبد الله فايد**- الحماية الجنائية للحياة الخاصة وبنوك المعلومات- دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩٢.

٣- **د/ جميل عبد الباقي الصغير**- الانترنت والقانون الجنائي- الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩.

٤- **د/ رمسيس بهنام**- النظرية العامة للقانون الجنائي- منشأة المعارف، ١٩٩٥.

٥- **د/ سامي على حامد عياد**- الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، ٢٠٠٧.

٦- **د/ سعيد عبد اللطيف حسن**- إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت- دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩.

٧- **د/ سليمان عبد المنعم**- النظرية العامة لقانون العقوبات- دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠.

٨- **د/ محمد سامي الشوا**- ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤.

٩- **د/ محمد على سكيكر**- الجريمة المعلوماتية وكيفية التصدي لها – مطابع دار الجمهورية للصحافة، أكتوبر ٢٠١٠.

١٠-**د/ نائل عبد الرحمن صالح** – جرائم الحاسوب في التشريع الأردني، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠.

١١-**د/ هشام محمد فريد رستم**- قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، ١٩٩٤.

١٢-**د/ هلالي عبد اللاه أحمد**– تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى، مطبعة دار النهضة العربية، الطبعة الأولي، القاهرة، ١٩٩٧.
-حجية المخرجات الكمبيوترية في المواد الجنائية– دراسة مقارنة، الطبعة الأولي، دار النهضة العربية، القاهرة، ١٩٩٧.

الرسائل العلمية:

١- **د/ ربيع محمود الصغير**– القصد الجنائي– دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٥.
٢- **د/ عمر محمد أبو بكر يونس**– الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، ٢٠٠٤.
٣- **د/ مروي السيد السيد الحصاوي**– مبدأ العالمية في القانون الجنائي– رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩.

الأبحـاث والمجـلات :

١- **د/ اشرف جابر سيد**– مسئولية مقدمي خدمات الانترنت عن المضمون الالكتروني غير المشروع (دراسة خاصة لمسئولية متعهدي الإيواء)– مجلة كلية الحقوق جامعة حلوان للدراسات القانونية والاقتصادية، العدد الثاني والعشرون، يناير – يوليو ٢٠١٠.
٢- **د/ تهاني السبيت** – ما هو البريد الالكتروني ، مقدمة دراسة منشورة على موقع الموسوعة العربية للكمبيوتر والانترنت، بتاريخ ٢٠٠١/١/٢١.
٣- **د/ جورج لبكي** – المعاهدات الدولية للانترنت – حقائق وتحديات، مجلة الدفاع الوطني، بحث منشور عبر الانترنت على موقع (http://www.lebarmy.gov.lb)
٤- **د/ صالح أحمد البربري** – دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٠٠١/١١/٢٣– بحث منشور عبر شبكة الانترنت بموقع الدليل الالكتروني للقانون العربي بتاريخ ٢٠٠٦/٩/٢. (www.arablawinfo.com)

٥- **د/ صالح سليمان عبد العظيم** – الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦ – ٢٨ سبتمبر ٢٠٠٤، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الإسلامي.
٦- **د/ علي حسن الطوالبه** – مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة– بحث منشور عبر الانترنت، مركز الإعلام الأمني، البحرين، ٢٠٠٩.
٧- **د/ ناول عبد الهادي**– تقييم فعاليات المواجهة التشريعية لجرائم الانترنت– مجلة العدل، المغرب، العدد٣١، رجب١٤٢٧.

القوانين والقرارات :

- الدستور المصري لجمهورية مصر لعربية الصادر عام ٢٠١٤ .
- قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، والمنشور بالجريدة الرسمية في العدد ٣٢ مكرر (ج) بتاريخ ٨/١٤ /٢٠١٨.
- اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات بموجب قرار مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ – المنشور بالجريدة الرسمية في العدد ٣٥ تابع (ج) – بتاريخ ٢٧ أغسطس سنة ٢٠٢٠ .
- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥.
- قانون مكافحة جرائم تقنية المعلومات الإماراتي الصادر بالمرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ وتعديلاته، المنشور بالجريدة الرسمية العدد ٤٥٠ ملحق السنة الثانية والأربعون – بتاريخ ٢٠١٢/٨/٢٦.
- نظام مكافحة جرائم المعلوماتية السعودي، الصادر بقرار مجلس الوزراء

رقم ٧٩ بتاريخ ٧/ ٣/ ١٤٢٨ هـ، والمصدق عليه بالمرسوم الملكي رقم ١٧م بتاريخ ١٤٢٨/٣/٨، والصادر بالقرار رقم ١١٥٦٧/ ب- بتاريخ ٩/ ٣/ ١٤٢٨ هـ.

- القرار بقانون رقم ١٥ لسنة ٢٠٠٤ الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ لسنة ٢٠٠٥- بشأن إصدار اللائحة التنفيذية لقانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
- قرار وزير الاتصالات ١٠٧ لسنة ٢٠٠٥ بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات.
- قرار وزير الاتصالات ١٢٨ لسنة ٢٠٠٦ بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات، وإنشاء إدارة تسمى (إدارة فض المنازعات) بالجهاز.
- قرار وزير الاتصالات رقم ١٠٨ لسنة ٢٠٠٥ بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات.

ثانيا: المراجع الأجنبية :

1- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 sur le commerce éléctronique, JOCE, n° L.178 du 17 juillet 2000.
2- Doan parker: Combattre la Criminalite informatique (paris, oros), 1985.
3- E.cesay: digital evidence and Computer Crim " londer, Academic press", 2000.
4- G. Haas et O. de Tissot, L'activité du fournisseur d'hébergement à l'epreuve des droits des tiers: Com. Comm. Électr. Juillet-août 2000, chron.
5- J. Passa, Propriété littéraire et artistique, internet et droit d'auteur, JCP Civil annexes, fasc. 1970.
6- Melanie Kowalski, «Cybercriminalité, enjeux, sources de données et faisabilité de recueillir des données auprès de la

police», Centre canadien de la statistique juridique, catalogue No 85-558-XIF, Décembre 2002.
http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85-558-XIF2002001.pdf.
7- Morgan Lavanchy, La responsabilité délictuelle sur Internet en droit Suisse, mém. 2002.
8- Mouhamad Chawki, Combattre LaCybercriminalite, Universite Lyon III, France, 2008.
9- Rapport de J. Cédras (avocat général à la Cour de Cassation) remis au Ministre de la Culture et de la Communication, Le téléchargement illicit d'oeuvres protégées par le droit d'auteur, avril 2007, cite par Simon Warynski, précité.
10- TOM Forester, Essential problèmes to High-tech Society First MIT Prés édition, Cambridge, Massachusetts, 1989.

الموضـــوع	رقم الصفحة
الآية القرآنية:	١
ملخص عربي:	٢
ملخص انجليزي:	٣
المُقــدمـــــــــــة:	٤-٨
المبحث الأول **نظرة عامة حول قانون تقنية المعلومات وضوابط التعاون الدولي**	٩-٩
المطلب الأول: ماهية جرائم تقنية المعلومات.	١٠
الفرع الأول: المقصود بتقنية المعلومات.	١٠
الفرع الثاني: المقصود بجرائم تقنية المعلومات.	١٣
المطلب الثاني: الجهود التشريعية المبذول لمكافحة الجريمة التقنية .	١٨
الفرع الأول: الجهود التشريعية الأوروبية .	١٩
الفرع الثاني: الجهود التشريعية العربية .	٢١
المطلب الثالث: ضوابط التعاون الدولي وتحديد الاختصاص القضائي.	٢٧
الفرع الأول: التعاون الدولي في مجال مكافحة الجريمة.	٢٨
الفرع الثاني: النطاق المكاني للقانون وتحديد الاختصاص القضائي .	٢٩
المبحث الثاني **أنماط الجرائم وحدود العقوبات المقررة لها**	٣٥-٣٦
المطلب الأول: جرائم الشبكات وأنظمة وتقنيات المعلومات.	٣٧
الفرع الأول: جرائم الدخول والانتفاع غير المشروع.	٣٨
الفرع الثاني: جرائم الاعتداء على البيانات والنظم المعلوماتية.	٤٦
الفرع الثالث: جرائم الاحتيال المالي والحيازة والاتجار غير المشروع بوسائل تقنية المعلومات.	٥٧
المطلب الثاني: الجرائم المتعلقة بالبريد الإلكتروني والمواقع أو الحسابات الخاصة.	٦٣
الفرع الأول: جرائم الاعتداء على بالبريد الإلكتروني والمواقع أو	٦٤

الحسابات الخاصة.	
الفرع الثاني: الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني.	٦٨
المطلب الثالث: جرائم الاعتداء على حرمة الحياة الخاصة وانتهاك الخصوصية.	٧٢
المبحث الثالث **الأحكام الإجرائية الخاصة بمكافحة الجرائم التقنية**	٧٩
المطلب الأول: إجراءات جمع الأدلة والاستدلالات التقنية.	٨٠-٨١
الفرع الأول: إجراءات الضبط والتفتيش.	٨٢
الفرع الثاني: إجراءات الاستعانة بالخبرة الفنية.	٨٧
الفرع الثالث: الحجية القانونية للأدلة الرقمية.	٩١
المطلب الثاني: التدابير والإجراءات التحفظية والعقوبات التبعية.	٩٦-٩٦
الفرع الأول : التدابير والإجراءات التحفظية.	٩٧
الغصن الأول: حجب المواقع الالكترونية والتظلم منها.	٩٧
الغصن الثاني: المنع من السفر وترقب الوصول.	١٠٢
الفرع الثاني : العقوبات التبعية أو التكميلية.	١٠٧
المطلب الثالث: الأحكام العامة المتعلقة بالعقوبـــة .	١١٢-١١٢
الفرع الأول: ضوابط التشديد والإعفاء من العقوبة.	١١٣
الفرع الثاني: أحكام الصلح والتصالح في الجريمة.	١١٧
الفرع الثالث: أحكام الشروع في الجريمة.	١٢٠
الفرع الرابع: أحكام المسئولية الجنائية .	١٢٢
الخاتمـــــة: النتائج: التوصيات:	١٣٢
قائمة المراجع:	١٣٧
الفهرس:	١٤١

The development of legislative policy in the field of combating information technology crimes

(Comparative analytical study)

Prepare

Dr. Hatem Ahmed Mohamed Batikh

PhD in Law - Ain Shams University

Associate Professor of Law at Egyptian